AVG AntiVirus Free Edition 2015

User Manual

Document revision 2015.18 (3.2.2015)

Copyright AVG Technologies CZ, s.r.o. All rights reserved.
All other trademarks are the property of their respective owners.

Contents

1. Introduction **3**

2. AVG Installation Requirements **4**

2.1 Operation Systems Supported 4

2.2 Minimum & Recommended Hardware Requirements 4

3. AVG Installation Process **5**

3.1 Welcome: Language selection 5

3.2 Welcome: License agreement 6

3.3 Select type of installation 7

3.4 Custom options 8

3.5 Install progress 9

3.6 Congratulations! 10

4. After Installation **11**

4.1 Product registration 11

4.2 Access to user interface 11

4.3 Scanning of the whole computer 11

4.4 Eicar test 11

4.5 AVG default configuration 12

5. AVG User Interface **13**

5.1 Upper Line Navigation 14

5.2 Security Status Info 16

5.3 Components Overview 17

5.4 My Apps 18

5.5 Scan / Update Quick Links 19

5.6 System Tray Icon 19

5.7 AVG Advisor 21

6. Components **22**

6.1 Computer protection 22

6.2 Web browsing protection 24

6.3 Identity protection 25

6.4 Email protection 26

6.5 PC Analyzer 28

7. AVG Security Toolbar **30**

8. AVG Do Not Track **32**

8.1 AVG Do Not Track interface 32

8.2 Information on tracking processes 34

8.3 Blocking tracking processes 34

8.4 AVG Do Not Track settings 35

9. AVG Advanced Settings **36**
9.1 Appearance 36
9.2 Sounds 38
9.3 Temporarily disable AVG protection 39
9.4 Computer Protection 40
9.5 Email Protection 44
9.6 Web Browsing Protection 53
9.7 Identity Protection 54
9.8 Scans 55
9.9 Schedules 60
9.10 Update 67
9.11 Exceptions 71
9.12 Virus Vault 72
9.13 AVG Self Protection 73
9.14 Privacy Preferences 73
9.15 Ignore Error Status 75
9.16 Advisor - Known Networks 75
10. AVG Scanning **77**
10.1 Predefined Scans 78
10.2 Scanning in Windows Explorer 87
10.3 Command Line Scanning 88
10.4 Scan Scheduling 91
10.5 Scan Results 97
10.6 Scan results details 98
11. AVG File Shredder **100**
12. Virus Vault **101**
13. History **102**
13.1 Scan results 102
13.2 Resident Shield Results 103
13.3 Identity Protection Results 106
13.4 Email Protection Results 107
13.5 Event History 108
14. AVG Updates **110**
14.1 Update launch 110
14.2 Update levels 110
15. FAQ and Technical Support **111**

1. Introduction

This user manual offers a general overview of the tasks and detection technologies provided by **AVG AntiVirus Free Edition 2015**. We will briefly talk about the program installation, initial startup, configuration and use.

AVG AntiVirus Free Edition 2015 is provided free-of-charge. It is up and running immediately from the moment of installation. All basic settings have been pre-set by the manufacturer, so most of the time you will not have to worry about anything – just let **AVG AntiVirus Free Edition 2015** work in the background and protect you without any effort on your part. However, there might be situations where you need to adjust the program settings, or decide what to do with a virus infected file; this manual is here to provide detailed information and assist you with any task.

You may also want to use other sources of information:

- ***Help file***: The help file included in **AVG AntiVirus Free Edition 2015** provides a list of most frequently occurring situations when a user desires to look up professional help to a technical issue. Please select the situation that best describes your problem, and click it to open detailed instructions leading to the problem solution.

- ***AVG website support center***: Alternatively, you can look up the solution to your problem on the AVG website (*http://www.avg.com/*). In the ***Support*** section you can find an overview of thematic groups dealing with both sales and technical issues, a structured section of frequently asked questions, and all available contacts.

- ***AVG ThreatLabs***: A specific AVG related website (*http://www.avg.com/about-viruses*) is dedicated to virus issues providing structured overview of information related to online threats. You can also find instructions on removing viruses, spyware, and advice on how to stay protected.

- ***Discussion forum***: You can also use the AVG Free users discussion forum at http://community.avg.com/.

2. AVG Installation Requirements

2.1. Operation Systems Supported

AVG AntiVirus Free Edition 2015 is intended to protect workstations with the following operating systems:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 and x64, all editions)
- Windows 7 (x86 and x64, all editions)
- Windows 8 (x32 and x64)

(and possibly higher service packs for specific operating systems)

***Note**: The Identity Protection component is not supported on Windows XP x64. On this operating system you can install AVG AntiVirus Free Edition 2015 but only without the IDP component.*

2.2. Minimum & Recommended Hardware Requirements

Minimum hardware requirements for **AVG AntiVirus Free Edition 2015** are as follows:

- Intel Pentium CPU 1.5 GHz or faster
- 1,2 GB of free hard drive space, for installation purposes
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7)

Recommended hardware requirements for **AVG AntiVirus Free Edition 2015** are as follows:

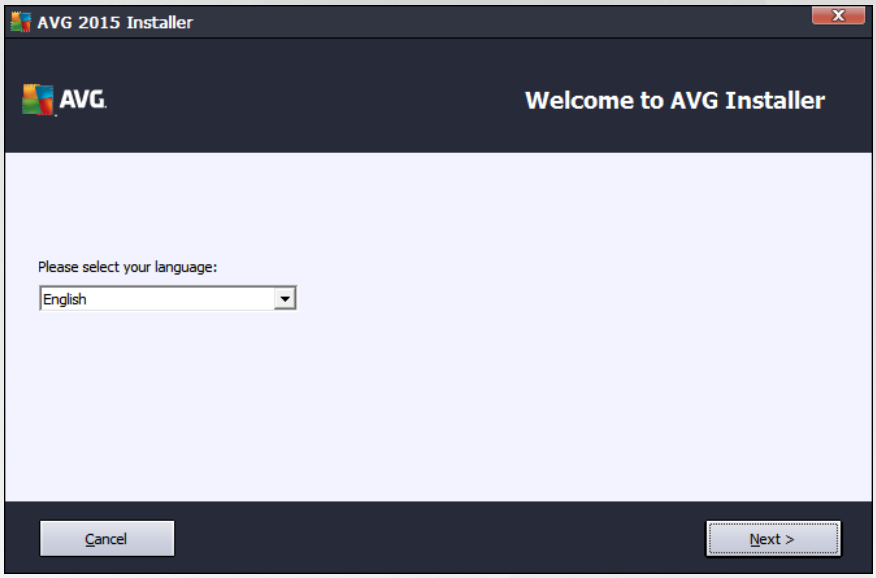
- Intel Pentium CPU 1.8 GHz or faster
- 1,5 GB of free hard drive space, for installation purposes
- 1024 MB of RAM memory

3. AVG Installation Process

To install **AVG AntiVirus Free Edition 2015** on your computer, you need to get the latest installation file. To make sure you are installing the up-to-date version of **AVG AntiVirus Free Edition 2015**, it is recommended that you download the installation file from the AVG Free website (http://free.avg.com/cz-en/homepage). Once you have downloaded and saved the installation file on your hard disk, you can launch the installation process. The installation is a sequence of simple and easy to understand dialogs. Each dialog briefly describes what do at each step of the installation process. We offer a detailed explanation of each dialog window below:

3.1. Welcome: Language selection

The installation process starts with the ***Welcome to AVG Installer*** dialog:

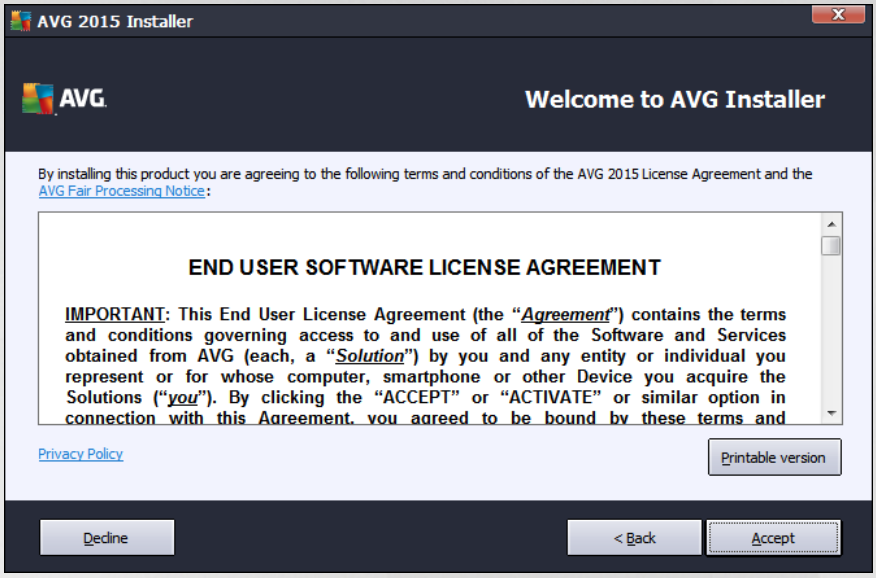


In this dialog you can select the language used for the installation process. Click the combo box to roll down the language menu. Select the desired language, and the installation process will proceed further in the language of your choice.

Attention: At the moment you are only selecting the language of the installation process. The AVG AntiVirus Free Edition 2015 application will be installed in the selected language, and in English which is always installed automatically. However, it is possible to have more languages installed and to work with AVG AntiVirus Free Edition 2015 in any of these. You will be invited to confirm your full selection of alternative languages in one of following setup dialogs named Custom Options.

3.2. Welcome: License agreement

The ***Welcome to AVG Installer*** dialog provides then the full wording of the AVG license agreement:


AVG 2015 Installer
AVG
Welcome to AVG Installer
By installing this product you are agreeing to the following terms and conditions of the AVG 2015 License Agreement and the AVG Fair Processing Notice:
END USER SOFTWARE LICENSE AGREEMENT
IMPORTANT: This End User License Agreement (the "Agreement") contains the terms and conditions governing access to and use of all of the Software and Services obtained from AVG (each, a "Solution") by you and any entity or individual you represent or for whose computer, smartphone or other Device you acquire the Solutions ("you"). By clicking the "ACCEPT" or "ACTIVATE" or similar option in connection with this Agreement, you agreed to be bound by these terms and
Privacy Policy
Printable version
Decline
< Back
Accept

Please read the entire text carefully. To confirm that you have read, understood, and accept the agreement press the ***Accept*** button. If you do not agree with the license agreement press the ***Decline*** button, and the installation process will be terminated immediately.

AVG Fair Processing Notice and Privacy Policy

Besides the license agreement, this setup dialog also offers you the option to learn more about ***AVG Fair Processing Notice***, and ***Privacy Policy***. The mentioned functions are displayed in the dialog in the form of an active hyperlink that takes you to the dedicated website where you can find detailed information. Click the respective link to get redirected to AVG website (http://www.avg.com/) where you can find the full wording of these statements.

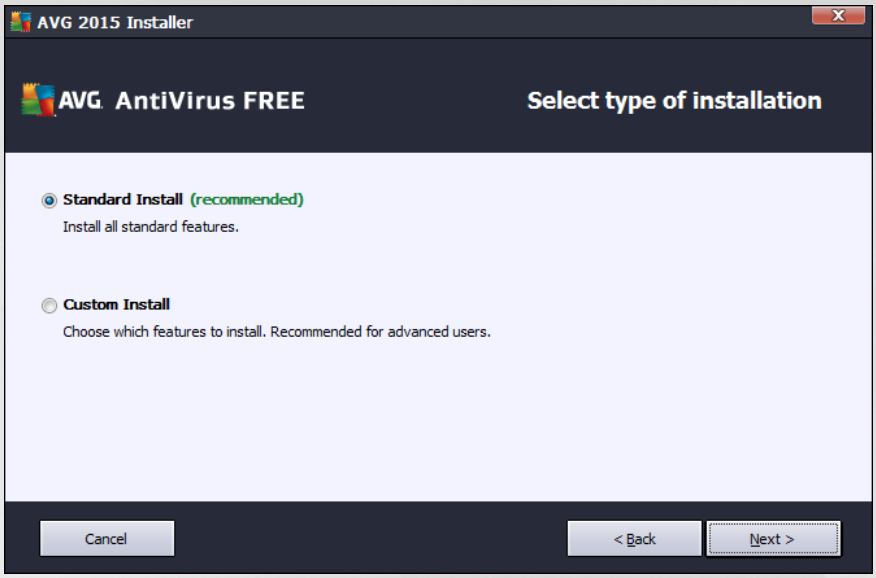
Control buttons

From the first setup dialog, the following control buttons are available:

- ***Printable version*** - Click the button to display the full wording of the AVG license agreement in a web interface, and well arranged for printing.
- ***Decline*** - click to refuse the license agreement. The setup process will quit immediately. **AVG AntiVirus Free Edition 2015** will not be installed!
- ***Back*** - click to go one step back to the previous setup dialog.
- ***Accept*** - click to confirm you have read, understood, and accepted the license agreement. The installation will continue, and you will go on one step further to the following setup dialog.

3.3. Select type of installation

The ***Select type of installation*** dialog offers the choice of two installation options: ***Standard*** and ***Custom Install***:



Standard installation

For most users, it is highly recommended that you keep the standard ***Standard*** installation. This way you install **AVG AntiVirus Free Edition 2015** in fully automatic mode with settings predefined by the program vendor. This configuration provides maximum security combined with the optimal use of resources. In the future, if the need arises to change the configuration, you will always have the option of doing so directly in the **AVG AntiVirus Free Edition 2015** application. Press the ***Next*** button to proceed to the following dialog of the installation process.

Custom installation

Custom Install should only be used by experienced users who have a valid reason to install **AVG AntiVirus Free Edition 2015** with non-standard settings; e.g. to fit specific system requirements. In this section you can select the destination folder, i.r. the location where **AVG AntiVirus Free Edition 2015** should be installed. By default, **AVG AntiVirus Free Edition 2015** will be installed to the program files folder located on drive C:, as stated in the text field in the dialog. If you want to change this location, use the ***Browse*** button to display the drive structure, and select the respective folder. To revert to the default destination pre-set by the software vendor use the ***Default*** button. Then, press the ***Next*** button to proceed to the Custom Options dialog.

Control buttons

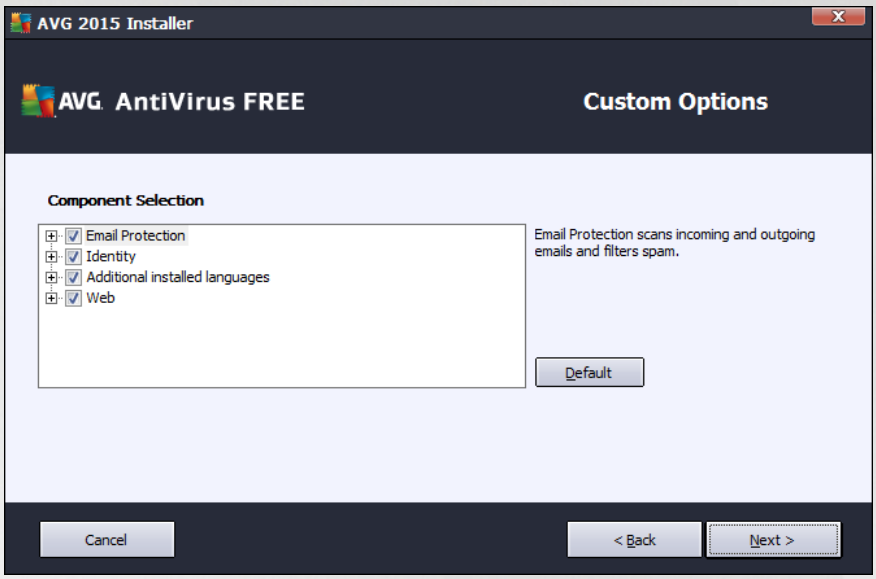
As within most setup dialogs, there are three control buttons available:

- ***Cancel*** - click to exit the setup process immediately; **AVG AntiVirus Free Edition 2015** will not be installed!

- ***Back*** - click to go one step back to the previous setup dialog.
- ***Next*** - click to continue the installation and go one step further.

3.4. Custom options

The ***Custom Options*** dialog allows you to set up detailed parameters for the installation:



The ***Component Selection*** section provides an overview of all **AVG AntiVirus Free Edition 2015** components that can be installed. If the default settings do not suit you, you can remove/add specific components. ***However, you can only select from components that are included in AVG AntiVirus Free Edition 2015!*** Highlight any item in the ***Component Selection*** list, and a brief description of the respective component will be displayed on the right side of this section. For detailed information on each component's functionality please consult the Components Overview chapter of this documentation. To revert to the default configuration previously set by the software vendor use the ***Default*** button.

In this step, you can also decide to install other then default language variants of the product *(by default, the application gets installed in the language you have selected as you setup communication language, and in English)*.

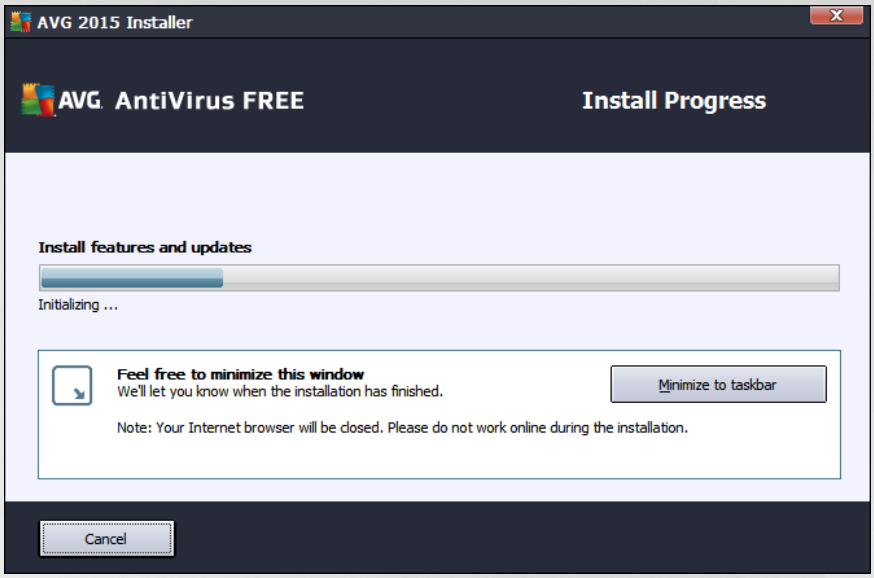
Control buttons

As in most setup dialogs, there are three control buttons available:

- ***Cancel*** - click to exit the setup process immediately; **AVG AntiVirus Free Edition 2015** will not be installed!
- ***Back*** - click to go one step back to the previous setup dialog.
- ***Next*** - click to continue the installation and go one step further.

3.5. Install progress

The ***Install Progress*** dialog shows the progress of the installation process, and does not require any intervention:


AVG 2015 Installer
AVG. AntiVirus FREE
Install Progress
Install features and updates
Initializing ...
Feel free to minimize this window
We'll let you know when the installation has finished.
Minimize to taskbar
Note: Your Internet browser will be closed. Please do not work online during the installation.
Cancel

After the installation process is finished, you will be automatically redirected to the next dialog.

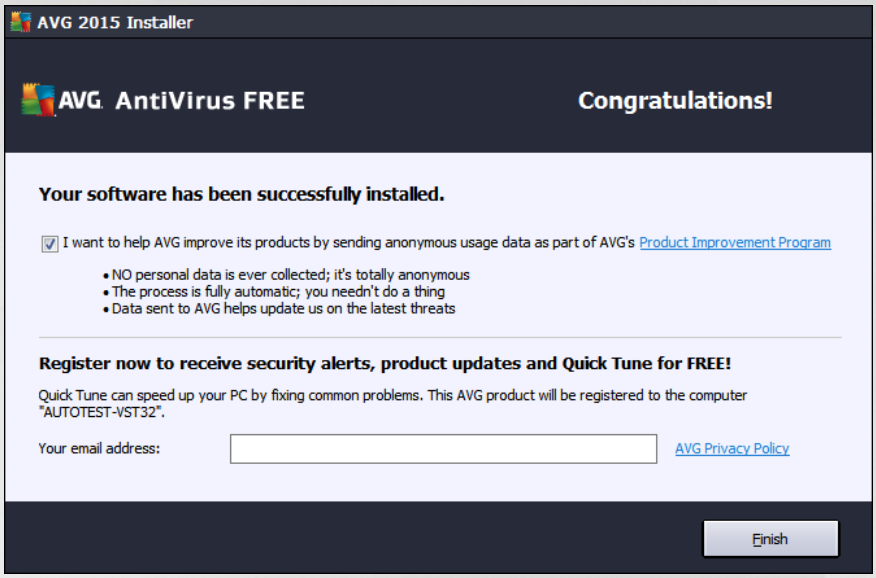
Control buttons

There are two control buttons available in this dialog:

- ***Minimize*** - The installation process may take several minutes. Click the button to minimize the dialog window into an icon visible on the system bar. The dialog appears again once the installation is completed.
- ***Cancel*** - This button should only be used if you want to stop the current installation process. Please mind that in such a case your **AVG AntiVirus Free Edition 2015** will not be installed!

3.6. Congratulations!

The ***Installation was successful*** dialog confirms that your **AVG AntiVirus Free Edition 2015** has been fully installed and configured:


AVG 2015 Installer
AVG. AntiVirus FREE
Congratulations!
Your software has been successfully installed.
I want to help AVG improve its products by sending anonymous usage data as part of AVG's Product Improvement Program
• NO personal data is ever collected; it's totally anonymous
• The process is fully automatic; you needn't do a thing
• Data sent to AVG helps update us on the latest threats
Register now to receive security alerts, product updates and Quick Tune for FREE!
Quick Tune can speed up your PC by fixing common problems. This AVG product will be registered to the computer "AUTOTEST-VST32".
Your email address:
AVG Privacy Policy
Finish

Product Improvement Program

Here you can decide whether you want to participate in the ***Product Improvement Program*** (*for details see the chapter AVG Advanced Settings / Product Improvement Program*) that collects anonymous information on detected threats in order to increase the overall Internet security level. All data are treated as confidential and in compliance with AVG Privacy Policy; click the ***Privacy Policy*** link to get redirected to AVG website (http://www.avg.com/) where you can find the the full wording of AVG Privacy Policy. If you agree, please keep the option checked *(the option is confirmed, by default)*.

Register now to receive security alerts, product updates and Quick Tune for FREE!

In case you would like to keep informed, please provide your email address so that we can provide you with news, information on program updates, security alerts, information on the current threat level, and send you relevant customer support news. However, providing your contact data is optional, and will be treated with full respect to the privacy policy.

Registered users can also use the ***Quick Tune*** service - an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved.

Control buttons

In the dialog, the only control button reads ***Finish***: click it to finalize the installation process, and enjoy the protection provided by **AVG AntiVirus Free Edition 2015**.

4. After Installation

4.1. Product registration

AVG AntiVirus Free Edition 2015 does not necessarily require registration. However, it is recommended that you register so that you can use the discussion forum of **AVG AntiVirus Free Edition 2015**, or rather in case you want to ask a question or react to one. For reading only the forum is accessible without registration. The easiest way to register is directly from the **AVG AntiVirus Free Edition 2015** user interface. Please select the Options / Register AVG. You will get redirected to the registration page of AVG Free Forum. Follow the instructions provided on the page to fill in the online registration form. Then you will receive the activation code via email sent to the provided email address, and you can log in to the forum.

4.2. Access to user interface

The AVG Free main dialog is accessible in several ways:

- double-click the AVG system tray icon
- double-click the AVG icon on the desktop
- from the menu ***Start / All Programs / AVG / AVG 2015***

4.3. Scanning of the whole computer

There is a potential risk that a computer virus has been transmitted to your computer prior to **AVG AntiVirus Free Edition 2015** installation. For this reason you should run a Scan of the whole computer to make sure there are no infections on your PC. The first scan might take quite some time *(about an hour)* but it is recommended that you launch it to make sure your computer has not been compromised by a threat. For instructions on running a Scan of the whole computer please consult the chapter AVG Scanning.

4.4. Eicar test

To confirm that **AVG AntiVirus Free Edition 2015** has been installed correctly you can perform the EICAR test.

The EICAR test is a standard and absolutely safe method used to test antivirus system operation. It is safe to pass around, because it is not an actual virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (*though they typically report it with an obvious name, such as "EICAR-AV-Test"*). You can download the EICAR virus from the EICAR website at www.eicar.com, and you will also find all necessary EICAR test information there.

Try to download the *eicar.com* file, and save it on your local disk. Immediately after you confirm downloading of the test file, your **AVG AntiVirus Free Edition 2015** will react to it with a warning. This notice demonstrates that AVG is correctly installed on your computer.

AVG AntiVirus FREE
AVG Detection
Threat: Virus identified EICAR_Test [More info]
Object name: c:\Users\Administrator\Documents\EICAR.COM
Protect Me (recommended)
AVG will choose the best method for removing this threat.
Ignore threat
AVG will prevent you from accessing the infected file. The threat will not be removed.
Show details

If **AVG AntiVirus Free Edition 2015** fails to identify the EICAR test file as a virus, you should check the program configuration again!

4.5. AVG default configuration

The default configuration (*i.e. how the application is set up right after installation*) of **AVG AntiVirus Free Edition 2015** is set by the software vendor so that all components and functions are tuned up to achieve optimum performance. ***Unless you have a real reason to do so, do not change the AVG configuration! Changes to settings should only be performed by an experienced user.*** If you want to change the AVG configuration to better suit your needs, go to AVG Advanced Settings: select the main menu item *Options/ Advanced settings*, and edit the AVG configuration in the newly opened AVG Advanced Settings dialog.

5. AVG User Interface

AVG AntiVirus Free Edition 2015 opens with the main window:

The main window is divided into several sections:

- ***Upper line navigation*** consists of four active links lined up in the upper section of the main window *(Like AVG, Reports, Support, Options).* Details >>
- ***Security Status Info*** provides basic information on the current status of your **AVG AntiVirus Free Edition 2015**. Details >>
- ***Installed components overview*** can be found in a horizontal strip of blocks in the central section of the main window. The components are displayed as light green blocks labeled by the respective component icon, and provided with the information on the component status. Details >>
- ***My Apps*** are graphically depicted in the lower central strip of the main window and offer you an overview of applications complementary to **AVG AntiVirus Free Edition 2015** that are either already installed on your computer, or recommended for installation. Details >>
- ***Scan / Fix / Update quick links*** are placed in the lower line of blocks in the main window. These buttons allow an immediate access to the most important and most frequently used AVG functions. Details >>

Outside the main window of **AVG AntiVirus Free Edition 2015**, there is one more control element that you might use to access the application:

- ***System tray icon*** is located in the bottom right-hand corner of the monitor *(on the system tray),* and indicates the current status of **AVG AntiVirus Free Edition 2015**. Details >>

5.1. Upper Line Navigation

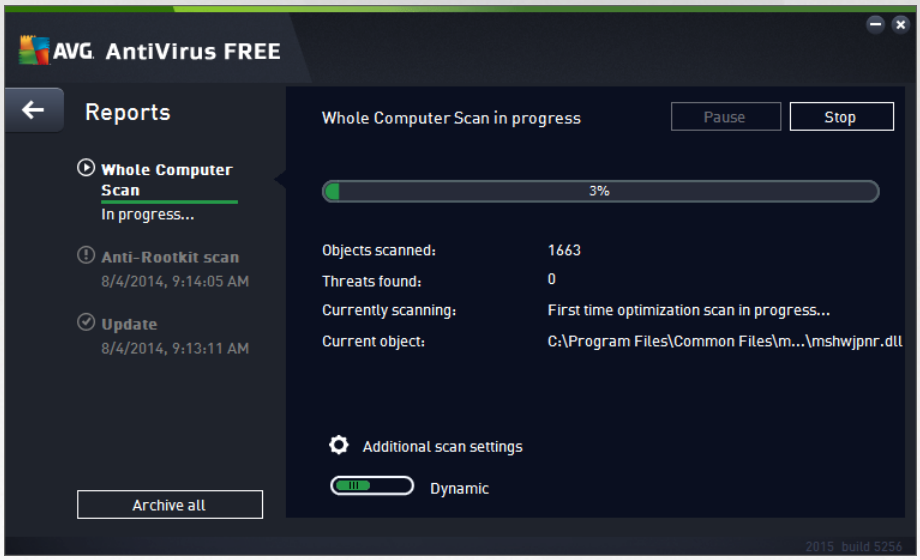
The ***Upper line navigation*** consists of several active links lined up in the upper section of the main window. The navigation includes the following buttons:

5.1.1. Join us on Facebook

Single click the link to get connected to the AVG Facebook community and to share the latest AVG information, news, tips and tricks for your maximum internet security.

5.1.2. Reports

Opens a new ***Reports*** dialog with an overview of all relevant reports on previously launched scans and update processes. If the scan or update is currently running, a rotating circle will be displayed next to the ***Reports*** text in the upper navigation of the main user interface. Click this circle to get to the dialog depicting the progress of the running process:



5.1.3. Support

Opens a new dialog structured into four tabs where you can find all relevant information about **AVG AntiVirus Free Edition 2015**:

- ***License and Support*** - The tab provides information on the product name, the license number, and the expiration date. In the bottom section of the dialog you can also find a clearly arranged overview of all available contacts to customer support. The following active links and buttons are available in the tab:

  - *(Re)Activate* - Click to open the new ***AVG Activate Software*** dialog. Fill in your license number into the respective field to either replace your sales number *(that you use during the AVG AntiVirus Free Edition 2015 installation)*, or to change your current license number for another *(e.g. when upgrading to a higher AVG product)*.

  - *Copy to clipboard* - Use this link to copy the license number, and paste it where needed. This way you can be sure the license number is entered correctly.

  - *Buy now* - You can buy a full professional licence of AVG directly on AVG website *(http://*

www.avg.com/) where you can find detailed information on all available programs.

- ***Product*** - The tab provides an overview of the **AVG AntiVirus Free Edition 2015** most important technical data referring to product information, installed components, installed email protection, and system information.
- ***Program*** - On this tab you can find information on the program file version, and on the third parties code used in the product.
- ***License Agreement*** - The tab offers the full wording of the license agreement between you and AVG Technologies.

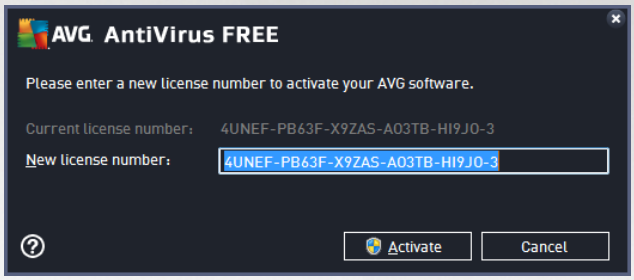
5.1.4. Options

The maintenance of **AVG AntiVirus Free Edition 2015** is accessible via the ***Options*** item. Click the arrow to open the roll-down menu:

- ***Scan computer*** - Switches to the AVG scanning interface and launches a scan of the whole computer.
- ***Scan selected folder...*** - Switches to the AVG scanning interface and allows you to define within the tree structure of your computer which files and folders should be scanned.
- ***Scan file...*** - Allows you to run an on-demand test over a single file selected from the tree structure of your disk.
- ***Update*** - Automatically launches the update process of **AVG AntiVirus Free Edition 2015.**
- ***Update from directory...*** - Runs the update process from the update files located in a specified folder on your local disk. However, this option is only recommended as an emergency, e.g. in situations where there is no connection to the Internet (*for example, your computer is infected and disconnected from the Internet; your computer is connected to a network with no access to the Internet, etc.*). In the newly opened window select the folder where you have previously placed the update file, and launch the update process.
- ***Virus Vault*** - Opens the interface to the quarantine space, Virus Vault, to where AVG removes all detected infections. Inside this quarantine the infected files are isolated, your computer's security is guaranteed, and at the same time the infected files are stored for possible future repair.
- ***History*** - Offers further specific submenu options:
  - *Scan results* - Opens a dialog providing an overview of scanning results.
  - *Resident Shield Results* - Opens a dialog with an overview of threats detected by Resident Shield.
  - *Identity Protection Results* - Opens a dialog with an overview of threats detected by Identity component.
  - *Email Scanner Results* - Opens a dialog with an overview of mail messages attachments detected as dangerous by the Email Protection component.
  - *Event history log* - Opens the history log interface with an overview of all logged **AVG AntiVirus**

Free Edition 2015 actions..

- ***Advanced settings...*** - opens the AVG advanced settings dialog where you can edit the **AVG AntiVirus Free Edition 2015** configuration. Generally, it is recommended that you keep the default settings of the application as defined by the software vendor.
- ***Help contents*** - Opens the AVG help files.
- ***Get support*** - Opens the support dialog providing all accessible contacts and support information..
- ***Your AVG Web*** - Opens ***AVG Free website*** *(http://free.avg.com/cz-en/homepage)*.
- ***About Viruses and Threats*** - Opens the ***AVG Free website*** *(http://free.avg.com/cz-en/homepage)* at the page dedicated to threats and viruses where you can look up detailed information on the identified virus.
- ***Buy now*** - Opens the AVG website *(http://www.avg.com/)* at the online store where you can purchase a copy of AVG.
- ***Activate*** - Opens the activation dialog with the data entered during the installation process. Within this dialog you can enter your new license number *(e.g. when upgrading to a paid AVG product)* to replace the AVG Free license number:



- ***Register AVG AntiVirus Free Edition 2015 / MyAccount*** - Opens ***AVG Free website*** *(http://free.avg.com/cz-en/homepage)* at the registration page where you can register to get the full access to a new web-based discussion forum where you can receive technical support.
- ***Premium Support*** - Opens you browser and takes you to AVG Support Center page, where you can select your product type to view all support options available for you.
- ***About AVG*** - Opens the ***AVG Information*** dialog with four tabs providing data on your purchased license and accessible support, product and program information, and the full wording of the license agreement. *(The same dialog can be opened via the Support link of the main navigation.)*

5.2. Security Status Info

The ***Security Status Info*** section is located in the upper part of the **AVG AntiVirus Free Edition 2015** main window. Within this section you will always find information on the current security status of your **AVG AntiVirus Free Edition 2015**. Please see an overview of icons possibly depicted in this section, and their meaning:

- The green icon indicates that your ***AVG AntiVirus Free Edition 2015 is fully functional***. Your computer is completely protected, up-to-date and all installed components are working properly.

- The yellow icon warns that ***one or more components are incorrectly configured*** and you should pay attention to their properties/settings. There is no critical problem in **AVG AntiVirus Free Edition 2015** and you have probably decided to switch some component off for some reason. You are still protected!. However, please pay attention to the problem component's settings! The incorrectly configured component will be displayed with a warning orange strip in the main user interface.

The yellow icon also appears if for some reason you have decided to ignore a component's error status. The ***Ignore error status*** option is accessible in the Advanced settings / Ignore error status branch. There you have the option to state you are aware of the component's error state but for some reason you wish to keep your **AVG AntiVirus Free Edition 2015** so and you do not want to be warned about it. You may need to use this option in a specific situation but it is strictly recommended that you switch the ***Ignore error status*** option off as soon as possible!

Alternatively, the yellow icon will also be displayed if your **AVG AntiVirus Free Edition 2015** requires the computer restart (***Restart needed***). Please pay attention to this warning and restart your PC.

- The orange icon indicates that ***AVG AntiVirus Free Edition 2015 is in a critical status***! One or more components do not work properly and **AVG AntiVirus Free Edition 2015** cannot protect your computer. Please pay immediate attention to fixing the reported problem!

In case AVG AntiVirus Free Edition 2015 is not set to the optimum performance, a new button named Click to fix (alternatively Click to fix it all if the problem involves more than one component) appears next to the security status information. Press the button to launch an automatic process of checking and configuring the program. This is an easy way to set AVG AntiVirus Free Edition 2015 to the optimum performance and reach the maximum security level!

It is strongly recommended that you pay attention to ***Security Status Info*** and in case the report indicates any problem, go ahead and try to solve it immediately. Otherwise your computer is at risk!

Note: *AVG AntiVirus Free Edition 2015 status information can also be obtained at any moment from the system tray icon.*

5.3. Components Overview

Installed components overview can be found in a horizontal strip of blocks in the central section of the main window. The components are displayed as light green blocks labeled by the respective component icon. Each block provides information on the current status of protection. If the component is configured correctly and fully functional, the information is stated in green letters. If the component is stopped, its functionality is limited, or the component is in error state, you will be notified by a warning text displayed in an orange text field. ***It is strictly recommended that you pay attention to the respective component's settings!***

Move the mouse over the component to display a short text at the bottom of the main window. The text provides an elementary introduction to the component's functionality. Also, it informs on the component's current status, and specifies which of the component's services is not configured correctly.

Installed components' list

Within the **AVG AntiVirus Free Edition 2015** the ***Components Overview*** section contains information on the following components:

- ***Computer*** - This component detects viruses, spyware, worms, trojans, unwanted executable files, or libraries within your system, and protects you from malicious adware. Details >>
- ***Web Browsing*** - Protects you from web-based attacks while you search and surf the Internet. Details >>
- ***Identity*** - The component constantly protects your digital assets from new and unknown threats on the Internet. Details >>
- ***Emails*** - Checks your incoming e-mail messages for SPAM, and blocks viruses, phishing attacks, or other threats. Details >>
- ***Firewall*** - Controls all communication on each network port, protecting you from malicious attacks and blocking all intrusion attempts. *However, Firewall is not activated in this edition, and is only accessible in a full professional version. Should you like to have access to further and extended functionality of AVG paid products; then please visit AVG website (http://www.avg.com/) for AVG purchase information.*

Actions accessible

- ***Move mouse over any component's icon*** to highlight it within the components overview. At the same time, the component's basic functionality description appears in the bottom part of the user interface.
- ***Single-click component's icon*** to open the component's own interface with the information on the component's current status, and access to its configuration and statistical data.

5.4. My Apps

In the ***My Apps*** area *(the line of green blocks under the components set)* you can find an overview of additional AVG applications that are either already installed on your computer, or recommended for installation. The blocks are displayed conditionally, and may represent any of the following applications:

- ***Mobile protection*** is an application that protects your cell phone from viruses and malware. It also provides you with the ability of tracking your smart phone remotely if you should become separated from it.
- ***LiveKive*** is dedicated to online data backup on secured servers. LiveKive automatically backs up all your files, photos, and music to one safe place, allowing you to share them with family and friends and access them from any web-enabled device, including iPhones and Android devices.
- ***Family Safety*** helps you protect your children from inappropriate websites, media content, and online searches, and provides you with reports regarding their online activity. AVG Family Safety uses key-stroke technology to monitor your child's activities in chat-rooms and on social networking sites. If it spots words, phrases or language that are known to be used to victimize children online, it will notify you immediately via SMS or email. The application allows you to set the appropriate level of protection for each of your children, and monitor them separately via unique logins.
- ***PC Tuneup*** application is an advanced tool for detailed system analysis and correction, as to how the speed and overall performance of your computer might be improved.

- ***AVG Toolbar*** is available directly in your Internet browser and guards your maximum security while browsing the Internet.

For detailed information on any of the ***My Apps*** applications click the respective block. You will get redirected to the dedicated AVG webpage, where you can also download the component immediately.

5.5. Scan / Update Quick Links

Quick links are located in the lower line of buttons in the **AVG AntiVirus Free Edition 2015** user interface. These links allow you to immediately access the most important and most frequently used features of the application, i.e. scanning and update. The quick links are accessible from all dialogs of the user interface:

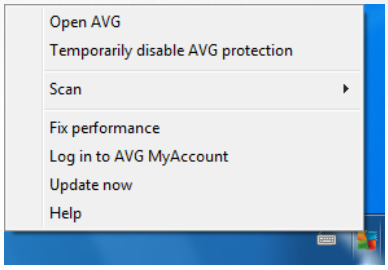
- ***Scan now*** - The button is graphically divided into two sections. Follow the ***Scan now*** link to launch the Whole Computer Scan immediately, and watch its progress and results in the automatically opened Reports window. The ***Options*** button opens the ***Scan Options*** dialog where you can manage scheduled scans and edit parameters of the Whole Computer Scan / Scan of Specific Files or Folders. *(For details see chapter AVG Scanning)*

- ***Fix performance*** - The button takes you to the ***PC Analyzer*** service, an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved.

- ***Update now*** - Press the button to launch the product update immediately. You will be informed about the update results in the slide dialog over the AVG system tray icon. *(For details see chapter AVG Updates)*

5.6. System Tray Icon

AVG System Tray Icon *(on your Windows taskbar, right-hand bottom corner of your monitor)* indicates the current status of your **AVG AntiVirus Free Edition 2015**. It is accessible at all times on your system tray, no matter whether the user interface of your **AVG AntiVirus Free Edition 2015** is opened or closed:



AVG System Tray Icon display

- In full color with no added elements the icon indicates that all **AVG AntiVirus Free Edition 2015** components are active and fully functional. However, the icon can also be displayed this way in a situation when one of the components is not fully functional but the user has decided to ignore the component state. *(Having confirmed the ignore the component state option you express you are aware of the component's error state but for some reason you wish to keep it so, and you do not want to be warned about the situation.)*

- The icon with an exclamation mark indicates that a component *(or even more components)* are in error state. Always pay attention to such a warning and try to remove the configuration issue of a component that is not set up properly. In order to be able to perform the changes in component's configuration, double-click the system tray icon to open the application user interface. For detailed information on which components is in error state please consult the security status info section.

- The system tray icon can further be displayed in full color with a flashing and rotating beam of light. This graphic version signalizes a currently launched update process.

- The alternative display of a full color icon with an arrow means that on of the **AVG AntiVirus Free Edition 2015** scans is just running.

AVG System Tray Icon information

AVG System Tray Icon further informs on current activities within your **AVG AntiVirus Free Edition 2015**, and on possible status changes in the program (*e.g. automatic launch of a scheduled scan or update, a component's status change, error status occurrence, ...*) via a pop-up window opened from the system tray icon.

Actions accessible from AVG System Tray Icon

AVG System Tray Icon can also be used as a quick link to access the user interface of **AVG AntiVirus Free Edition 2015**, just double-click on the icon. By right-click on the icon you open a brief context menu with the following options:

- ***Open AVG*** - Click to open the user interface of **AVG AntiVirus Free Edition 2015**.

- ***Temporarily disable AVG protection*** - The option allows you to switch off the entire protection secured by your **AVG AntiVirus Free Edition 2015** at once. Please remember that you should not use this option unless it is absolutely necessary! In most cases, it is not necessary to disable **AVG AntiVirus Free Edition 2015** before installing new software or drivers, not even if the installer or software wizard suggests that running programs and applications be shut down first to make sure there are no unwanted interruptions during the installation process. If you do have to temporarily disable **AVG AntiVirus Free Edition 2015**, you should re-enable it as soon as you're done. If you are connected to the Internet or a network during the time your antivirus software is disabled, your computer is vulnerable to attacks.

- ***Scan*** - Click to open the context menu of predefined scans (*Whole Computer scan*, *Scan Specific Files or Folders*, *and Anti-Rootkit scan*) and select the required scan, it will be launched immediately.

- ***Running scans*** - This item is displayed only in case a scan is currently running on your computer. For this scan you can then set its priority, alternatively stop or pause the running scan. Further, the following actions are accessible: *Set priority for all scans, Pause all scans* or *Stop all scans*.

- ***Fix performance*** - Launches the PC Analyzer component.

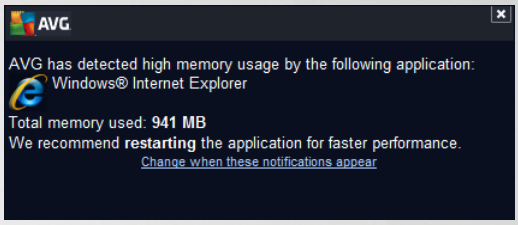
- ***Log in to AVG MyAccount*** - Opens the MyAccount homepage where you can manage your subscription products, purchase additional protection, download installation files, check your past orders and invoices, and manage your personal information.

- ***Update now*** - Launches an immediate update.
- ***Help*** - Opens the help file on the start page.

5.7. AVG Advisor

AVG Advisor has been designed to detect problems that might be slowing your computer down, or putting it at risk, and to recommend an action to solve the situation. If you see a sudden computer slowdown *(Internet browsing, overall performance)*, it is not usually obvious what exactly the culprit is, and subsequently, how to solve the problem. That is where ***AVG Advisor*** comes in: It will display a notification in the system tray informing you what the problem might be, and suggesting how to fix it. ***AVG Advisor*** keeps monitoring all running processes within your PC for possible issues, and offering tips on how to avoid the problem.

AVG Advisor is visible in the form of a sliding pop-up over the system tray:


AVG
AVG has detected high memory usage by the following application:
Windows® Internet Explorer
Total memory used: 941 MB
We recommend restarting the application for faster performance.
Change when these notifications appear

Specifically, ***AVG Advisor*** monitors the following:

- ***The state of any currently opened web browser***. Web browsers may overload the memory, especially if multiple tabs or windows have been opened for some time, and consume too much of system resources, i.e. slowing down your computer. In such situation, restarting the web browser usually helps.
- ***Running Peer-To-Peer connections***. After using the P2P protocol for sharing files, the connection can sometimes remain active, using up certain amount of your bandwidth. As a result, you can see web browsing slowdown.
- ***Unknown network with a familiar name***. This usually only applies to users who connect to various networks, typically with portable computers: If a new, unknown network has the same name as a well-known, frequently used network *(e.g. Home or MyWifi)*, confusion can occur, and you can accidentally connect to a completely unknown and potentially unsafe network. ***AVG Advisor*** can prevent this by warning you that the known name actually represents a new network. Of course, if you decide that the unknown network is safe, you can save it to an ***AVG Advisor*** list of known networks so that it is not reported again in the future.

In each of these situation, ***AVG Advisor*** warns you of the possible problem that might occur, and it provides the name and icon of the conflicting process, or application. Also, ***AVG Advisor*** suggests what steps should be taken to avoid the possible problem.

Supported web browsers

The feature works with the following web browsers: Internet Explorer, Chrome, Firefox, Opera, Safari.

6. Components

6.1. Computer protection

The ***Computer Protection*** component covers two main security services: ***AntiVirus*** and ***Data Safe***. In the **AVG AntiVirus Free Edition 2015**, the ***Computer Protection*** component offers just the ***AntiVirus*** part. The ***Data Safe*** is not activated in this edition, and is only accessible in a full professional version. Should you like to have access to further and extended functionality of AVG paid products; then please visit AVG website *(http://www.avg.com/)* for AVG purchase information.

- ***AntiVirus*** consists of a scanning engine that guards all files, the system areas of the computer, and removable media *(flash disk etc.)* and scans for known viruses. Any detected virus will be blocked from taking any action, and will then be cleaned or quarantined in the Virus Vault. You do not even notice the process, as this so called resident protection runs "in the background". AntiVirus also uses heuristic scanning, where files are scanned for typical virus characteristics. This means that the AntiVirus can detect a new, unknown virus, if the new virus contains some typical characteristics of existing viruses. **AVG AntiVirus Free Edition 2015** is also able to analyze and detect executable applications or DLL libraries that could be potentially unwanted within the system *(various kinds of spyware, adware etc.)*. Furthermore, AntiVirus scans your system registry for suspicious entries, temporary Internet files, and tracking cookies, and allows you to treat all potentially unwanted items in the same way as any other infection.

- ***Data Safe*** enables you to create secure virtual vaults to store valuable or sensitive data in. The contents of a Data Safe are encrypted and protected with a password of your choice so that nobody can access it without authorization. *Unfortunately, in AVG AntiVirus Free Edition 2015 the Data Safe service is not included. If you like to use this type of protection, please visit the AVG website (http://www.avg.com/) for AVG purchase and upgrade information.*

Dialog controls

To switch between both sections of the dialog, you can simply click anywhere in the respective service panel. The panel then gets highlighted in a lighter shade of blue. In both sections of the dialog you can find the following controls. Their functionality is the same whether they belong to one security service or another *(AntiVirus or Data Safe)*:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the AntiVirus security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. AntiVirus. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus Free Edition 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

Unfortunately, in **AVG AntiVirus Free Edition 2015** the ***Data Safe*** service is not included. If you like to use

this type of protection, visit the dedicated AVG website (*http://www.avg.com/*) for AVG purchase information.

6.2. Web browsing protection

In the **AVG AntiVirus Free Edition 2015**, the ***Web Browsing Protection*** component offers just the ***LinkScanner*** service. The ***Online Shield*** is not activated in this edition, and is only accessible in a full professional version. Should you like to have access to further and extended functionality of AVG paid products; then please visit AVG website *(http://www.avg.com/)* for AVG purchase information.

- ***LinkScanner*** protects you from the increasing number of 'here today, gone tomorrow' threats on the web. These threats can be hidden on any type of website, from governments to big, well-known brands to small businesses, and they rarely stick around on those sites for more than 24 hours. LinkScanner protects you by analyzing the web pages behind all the links on any web page you're viewing and making sure they're safe at the only time that matters - when you're about to click that link. ***LinkScanner is not intended for server platforms protection!***

- ***Online Shield*** *(not activated within AVG AntiVirus Free Edition 2015)* is a type of a real time resident protection; it scans the content of visited web pages (and possible files included in them) even before these are displayed in your web browser or downloaded to your computer. Online Shield detects that the page you are about to visit includes some dangerous javascript, and prevents the page from being displayed. Also, it recognizes malware contained in a page and stops its downloading immediately so that it never gets to your computer. This powerful protection will block malicious content of any web page you try to open, and prevent it from being downloaded to your computer. With this feature enabled, clicking a link or typing in a URL to a dangerous site will automatically block you from opening the web page thus protecting you from inadvertently being infected. It is important to remember that exploited web pages can infect your computer simply by visiting the affected site. ***Online Shield is not intended for server platforms protection!***

Dialog controls

To switch between both sections of the dialog, you can simply click anywhere in the respective service panel. The panel then gets highlighted in a lighter shade of blue. In both sections of the dialog you can find the following controls. Their functionality is the same whether they belong to one security service or another *(however, only LinkScanner service is activated)*:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the LinkScanner Surf-Shield / Online Shield security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. LinkScanner Surf-Shield. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus Free Edition 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

Unfortunately, in **AVG AntiVirus Free Edition 2015** the Online Shield service is not included. If you like to use this type of protection, follow the ***GO PRO*** button to get redirected to the dedicated AVG website (*http://www.avg.com/*) for AVG purchase information.

6.3. Identity protection

Identity Protection is an anti-malware service that protects you from all kinds of malware (*spyware, bots, identity theft, ...*) using behavioral technologies and provide zero day protection for new viruses. Identity Protection is focused on preventing identity thieves from stealing your passwords, bank account details, credit card numbers and other personal digital valuables from all kinds of malicious software *(malware)* that target your PC. It makes sure that all programs running on your PC or in your shared network are operating correctly. Identity Protection spots and blocks suspicious behavior on a continuous basis and protects your computer from all new malware. Identity Protection gives your computer a realtime protection against new and even unknown threats. It monitors all *(including hidden)* processes and over 285 different behaviour patterns, and can determine if something malicious is happening within your system. For this reason, it can reveal threats not even yet described in the virus database. Whenever an unknown piece of code comes onto your computer, it is immediately watched for malicious behaviour, and tracked. If the file is found to be malicious, Identity Protection will remove the code into the Virus Vault and undo any changes that have been made to the system *(code injections, registry changes, ports opening etc)*. You do not need to initiate a scan to be protected. The technology is very proactive, rarely needs updating, and is always on guard.

Dialog controls

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the Identity Protection security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. Identity Protection. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus Free Edition 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

6.4. Email protection

In the **AVG AntiVirus Free Edition 2015**, the ***Email protection*** component offers just the ***Email Scanner*** service. The ***Anti-Spam*** is not activated in this edition, and is only accessible in a full professional version. Should you like to have access to further and extended functionality of AVG paid products; then please visit

AVG website (http://www.avg.com/) for AVG purchase information.

- ***Email Scanner***: One of the most common sources of viruses and trojans is via email. Phishing and spam make email an even greater source of risks. Free email accounts are more likely to receive such malicious emails *(as they rarely employ anti-spam technology)*, and home users rely quite heavily on such email. Also home users, surfing unknown sites and filling in online forms with personal data *(such as their email address)*, increase exposure to attacks via email. Companies usually use corporate email accounts and employ anti-spam filters etc, to reduce the risk. The Email Protection component is responsible for scanning every email message sent or received; whenever a virus is detected in an email, it is removed to the Virus Vault immediately. The component can also filter out certain types of email attachments, and add a certification text to infection-free messages. ***Email Scanner is not intended for server platforms!***

- ***Anti-Spam*** *(not activated within AVG AntiVirus Free Edition 2015)* checks all incoming email messages and marks unwanted emails as spam *(Spam refers to unsolicited email, mostly advertising a product or service that is mass mailed to a huge number of email addresses at the same time, filling recipients' mail boxes. Spam does not refer to legitimate commercial email for which consumers have given their consent.)*. Anti-Spam can modify the subject of the email *(that has been identified as spam)* by adding a special text string. You can then easily filter your emails in your email client. The Anti-Spam component uses several analysis methods to process each email message, offering maximum possible protection from unwanted email messages. Anti-Spam uses a regularly updated database for the detection of spam. It is also possible to use RBL servers *(public databases of "known spammer" email addresses)* and to manually add email addresses to your whitelist *(never mark as spam)* and blacklist *(always mark as spam)*.

Dialog controls

To switch between both sections of the dialog, you can simply click anywhere in the respective service panel. The panel then gets highlighted in a lighter shade of blue. In both sections of the dialog you can find the following controls. Their functionality is the same whether they belong to one security service or another *(however, only Email Scanner service is activated)*:

Enabled / Disabled - The button may remind you of a traffic light, both in appearance and in functionality. Single click to switch between two positions. The green color stands for ***Enabled***, which means that the security service is active and fully functional. The red color represents the ***Disabled*** status, i.e. the service is deactivated. If you do not have a good reason to deactivate the service, we strictly recommend that you keep the default settings for all security configuration. The default settings guarantees the optimum performance of the application, and your maximum security. If for some reason you wish to deactivate the service, you will be warned about the possible risk immediately by the red ***Warning*** sign and the information that you are not fully protected at the moment. ***Please mind, that you should activate the service again as soon as possible!***

Within the Email Scanner section you can see two of "traffic light" buttons. This way you can separately specify whether you want to have the Email Scanner checking the incoming, or outgoing messages, or both. By default, the scanning is on for incoming messages while off for outgoing mail where the risk of infection is rather low.

Settings - Click the button to get redirected to advanced settings interface. Precisely, the respective dialog opens and you will be able to configure the selected service, i.e. Email Scanner. In the advanced settings interface you can edit all configuration of each security service within **AVG AntiVirus Free Edition 2015** but any configuration can be recommended to experienced users only!

Arrow - Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

Unfortunately, in **AVG AntiVirus Free Edition 2015** the Anti-Spam service is not included. If you like to use this type of protection, follow the ***GO PRO*** button to get redirected to the dedicated AVG website (*http://www.avg.com/*) for AVG purchase information.

6.5. PC Analyzer

The ***PC Analyzer*** component is an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved. It opens via the ***Fix performance*** button located in the main user interface dialog or via the same option listed in the context menu of the system tray AVG icon. You will then be able to watch the analysis progress and its results directly in the chart:

The following categories can be analyzed: registry errors, junk files, fragmentation, and broken shortcuts:

- ***Registry Errors*** will give you the number of errors in Windows Registry that might be slowing your computer down, or causing error messages to appear.
- ***Junk Files*** will give you the number of files that use up your disk space, and can most likely be deleted. Typically, these will be many kinds of temporary files, and files in the Recycle Bin.
- ***Fragmentation*** will calculate the percentage of your hard disk that is fragmented, i.e. used for a long time so that most files are now scattered over different parts of the physical disk.
- ***Broken Shortcuts*** will find shortcuts that no longer work, lead to non-existing locations etc.

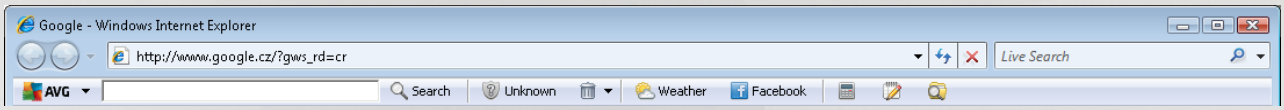
The results overview provides the number of detected system problems classified according to the respective categories tested. The analysis results will also be displayed graphically on an axis in the ***Severity*** column.

Control buttons

- ***Stop analysis*** (*displayed while the analysis is running*) - Press this button to interrupt the analysis of your computer.
- ***Fix now*** *(displayed once the analysis is finished*) - Unfortunately, the functionality of the PC Analyzer within the **AVG AntiVirus Free Edition 2015** is limited to your PC present status analysis. However, within the paid versions, AVG provides an advanced tool for detailed system analysis and correction for how the speed and overall performance of your computer might be improved. Click the button to get redirected to the dedicated website for more information.

7. AVG Security Toolbar

AVG Security Toolbar is a tool that closely cooperates with the LinkScanner Surf-Shield service, and guards your maximum security while browsing the Internet. Within **AVG AntiVirus Free Edition 2015**, the installation of ***AVG Security Toolbar*** is optional; during the installation process you were invited to decide whether the component should be installed. ***AVG Security Toolbar*** is available directly in your Internet browser. At the moment, the supported Internet browsers are Internet Explorer (*version 6.0 and higher*), and/or Mozilla Firefox (*version 3.0 and higher*). No other browsers are supported *(in case you are using some alternative Internet browser, e.g Avant Browser, you may encounter unexpected behavior).*



AVG Security Toolbar consists of the following items:

- ***AVG logo*** with the drop-down menu:
  - ***Current Threat Level*** - opens the virus lab web page with a graphical display of the current threat level on the web.
  - ***AVG Threat Labs*** - opens the specific ***AVG Threat Lab*** website *(at http://www.avgthreatlabs.com)* where you can find information on various websites security and the current threat level online.
  - ***Toolbar Help*** - opens the online help covering all ***AVG Security Toolbar*** functionality.
  - ***Submit Product feedback*** - opens a web page with a form that you can fill in and tell us how you feel about the ***AVG Security Toolbar***.
  - ***End User License Agreement*** - opens the AVG website at page providing the full wording of the license agreement related to use of your **AVG AntiVirus Free Edition 2015**.
  - ***Privacy Policy*** - opens the AVG website at page where you can find the the full wording of AVG Privacy Policy.
  - ***Hide / uninstall AVG Toolbar*** - opens a web page providing a detailed description of how to deactivate the ***AVG Security Toolbar*** in each of the supported web browsers.
  - ***About...*** - opens a new window with the information on the currently installed ***AVG Security Toolbar*** version.
- ***Search field*** - search the Internet using the ***AVG Security Toolbar*** to be absolutely secure and comfortable since all displayed search results are hundred percent safe. Fill in the keyword or a phrase into the search field, and press the ***Search*** button *(or Enter)*.
- ***Site Safety*** - this button opens a new dialog providing information on the current threat level (*Safe*) of the page you are just visiting. This brief overview can be expanded, and displayed with full details of all security activities related to the page right within the browser window (*Full Website Report*):

- ***Do Not Track*** - the DNT service helps you identify websites that are collecting data about your online activities, and gives you the choice to allow or disallow it. Details >>

- ***Delete*** - the 'trash bin' button offers a roll down menu where you can select whether you want to delete information on your browsing, downloads, online forms, or delete all of your search history at once.

- ***Weather*** - the button opens a new dialog providing information on the current weather in your location, and the weather forecast for the next two days. This information is updated regularly, every 3-6 hours. In the dialog, you can change the desired location manually, and decide whether you want to see the temperature info in Celsius or Fahrenheit.

- ***Facebook*** - This buttons allows you connect to the Facebook social network directly from within the ***AVG Security Toolbar***.

- Shortcut buttons for quick access to these applications: ***Calculator***, ***Notepad***, ***Windows Explorer***.

8. AVG Do Not Track

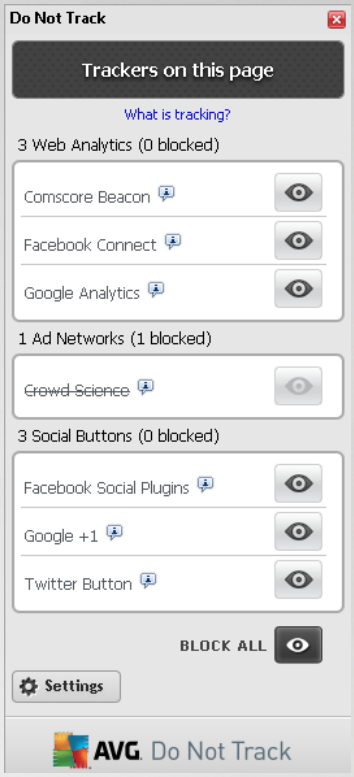
AVG Do Not Track helps you identify websites that are collecting data about your online activities. The ***AVG Do Not Track*** that is a part a AVG Security Toolbar shows the websites or advertisers collecting data about your activity and gives you the choice to allow or disallow it.

- ***AVG Do Not Track*** provides you with additional information about privacy policy of each respective service as well as a direct link to Opt-out from the service, if that is available.
- In addition, ***AVG Do Not Track*** supports the W3C DNT protocol to automatically notify sites that you don't want to be tracked. This notification is enabled by default, but can be changed at any time.
- ***AVG Do Not Track*** is provided under these terms and conditions.
- ***AVG Do Not Track*** is disabled by default. For more information please consult the FAQ article How to disable or configure AVG Do Not Track.
- For more information on ***AVG Do Not Track***, please visit our website.

Currently, the ***AVG Do Not Track*** functionality is supported in Mozilla Firefox, Chrome, and Internet Explorer browsers.

8.1. AVG Do Not Track interface

While online, ***AVG Do Not Track*** warns you as soon as any kind of data collection activity is detected. In such a case, the ***AVG Do Not Track*** icon located at the AVG Security Toolbar changes its look; a small number appears by the icon providing information on a number of detected data collection services: Click the icon to see the following dialog:



All detected data collection services are listed in the ***Trackers on this page*** overview. There are three types of data collection activities recognized by ***AVG Do Not Track***:

- ***Web Analytics*** *(allowed by default):* Services used to improve the performance and experience of the respective website. In this category you can find services as Google Analytics, Omniture, or Yahoo Analytics. We recommend not to block web analytics services, as the website might not work as intended.
- ***Ad Networks*** *(some blocked by default):* Services that collect or share data about your online activity on multiple sites, either directly or indirectly, to offer you personalized Ads unlike of content-based Ads. This is determined based on the privacy policy of each Ad network as available on their website. Some ad networks are blocked by default.
- ***Social Buttons*** *(allowed by default):* Elements designed for improving the social-networking experience. Social buttons are served from the social networks to the site you are visiting. They can collect data about your online activity while you are logged-in. Examples of Social buttons include: Facebook Social Plugins, Twitter Button, Google +1.

Note: *Depending on what services are running in the background of the website, some of the three above described sections might not appear in the AVG Do Not Track dialog.*

Dialog controls

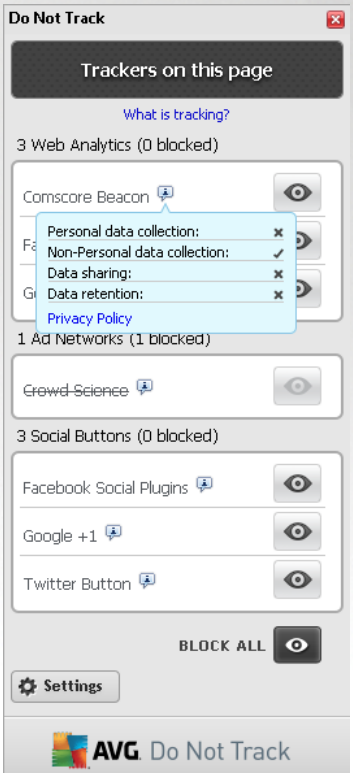
- ***What is tracking?*** - Click this link in the upper section of the dialog to get redirected to the dedicated webpage providing detailed explanation on the tracking principles, and description of specific tracking types.

- ***Block All*** - Click the button located in the bottom section of the dialog to to say you do not wish any data collection activity at all *(for details see chapter Blocking tracking processes).*

- ***Do Not Track settings*** - Click this button in the bottom section of the dialog to get redirected to the dedicated webpage where you can set the specific configuration of various ***AVG Do Not Track*** parameters *(see the AVG Do Not Track settings chapter for detailed information)*

8.2. Information on tracking processes

The list of detected data collection services provides just the name of the specific service. To make a conversant decision about whether the respective service should be blocked or allowed, you may need to know more. Move your mouse over the respective list item. An information bubble appears providing detailed data on the service. You will learn whether the service collects personal data, or other data available; whether the data are being shared with other third party subjects, and whether the collected data are being filed for possible further use:



In the lower section of the information bubble you can see the ***Privacy Policy*** hyperlink that redirects you to the website dedicated to privacy policy of the respective detected service.

8.3. Blocking tracking processes

With the lists of all Ad Networks / Social Buttons / Web Analytics you have now the option to control which services should be blocked. You can go two ways:

- ***Block All*** - Click this button located in the bottom section of the dialog to to say you do not wish any data collection activity at all. *(However, please keep in mind that this action may break functionality in the respective webpage where the service is running!)*

- - If you do not want to block all the detected services at once, you can specify whether the service should be allowed or blocked individually. You may allow running of some of the detected systems *(e.g. Web Analytics):* these systems use the collected data for their own website optimization, and this way they help to improve the common Internet environment for all users. However, at the same time you may block the data collection activities of all processes classified as Ad Networks. Just click the icon next to the respective service to block the data collection *(the process name will appear as crossed out)*, or to allow the data collection again.

8.4. AVG Do Not Track settings

The ***Do Not Track Options*** dialog offers the following configuration options:

- ***Do Not Track is enabled*** - By default, the DNT service is active *(switch ON)*. To disable the service, move the switch to the OFF position.

- In the central section of the dialog you can see a box with a list of known data collection services that can be classified as Ad Networks. By default, ***Do Not Track*** blocks some of Ad Networks automatically and it remains up to your decision whether the rest should be blocked as well, or left allowed. To do so, just click the ***Block All*** button under the list. Or, you may use the ***Defaults*** button to cancel all performed settings changes, and to return to the original configuration.

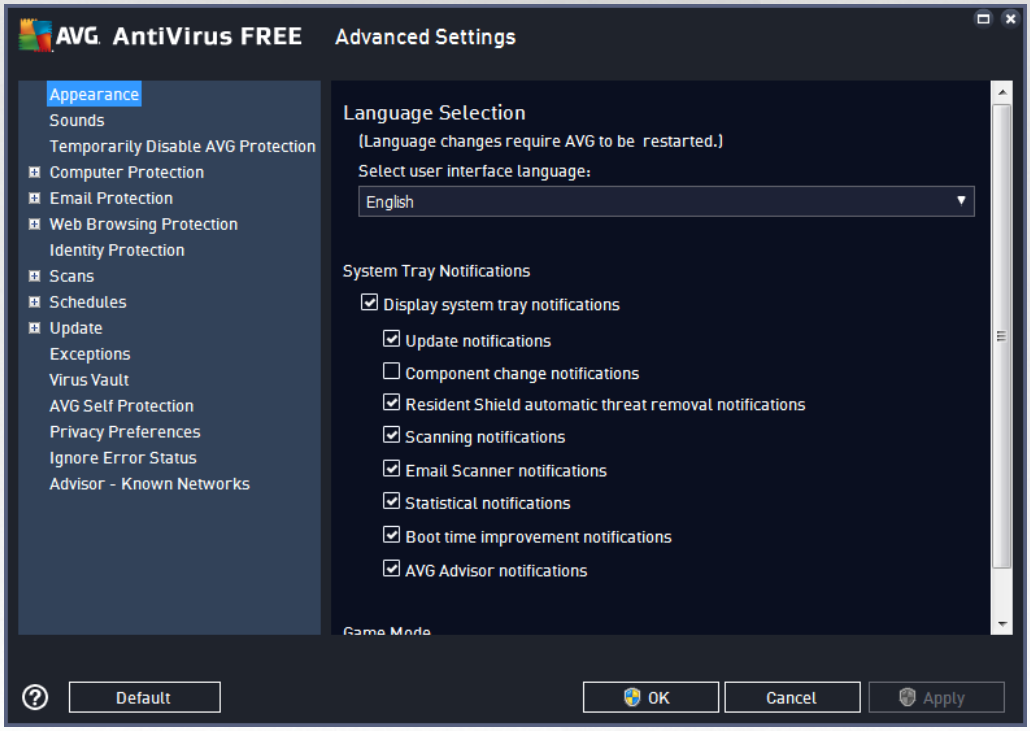
- ***Notify web sites ...*** - In this section you can switch on/off the ***Notify web sites that I do not want to be tracked*** option *(on by default).* Keep this option marked to confirm that you want ***Do Not Track*** to inform the provider of a detected data collection service that you do not want to be tracked.

9. AVG Advanced Settings

The advanced configuration dialog of **AVG AntiVirus Free Edition 2015** opens in a new window named ***Advanced AVG Settings***. The window is divided into two sections: the left part offers a tree-arranged navigation to the program configuration options. Select the component you want to change the configuration of (*or its specific part*) to open the editing dialog in the right-hand section of the window.

9.1. Appearance

The first item of the navigation tree, ***Appearance***, refers to the general settings of the **AVG AntiVirus Free Edition 2015** user interface, and provides a few elementary options of the application's behavior:



Language selection

In the ***Language selection*** section you can chose your desired language from the drop-down menu. The selected language will then be used for the entire **AVG AntiVirus Free Edition 2015** user interface. The drop-down menu only offers those languages you have previously selected to be installed during the installation process plus English (*English is always installed automatically, by default*). To finish switching your **AVG AntiVirus Free Edition 2015** to another language you have to restart the application. Please follow these steps:

- In the drop-down menu, select the desired language of the application
- Confirm your selection by pressing the ***Apply*** button *(right-hand bottom corner of the dialog)*
- Press the ***OK*** button confirm
- A new dialog pops-up informing you that in order to change the language of the application, you need

to restart your **AVG AntiVirus Free Edition 2015**

- Press the ***Restart the application now*** button to agree with the program restart, and wait a second for the language change to take effect:

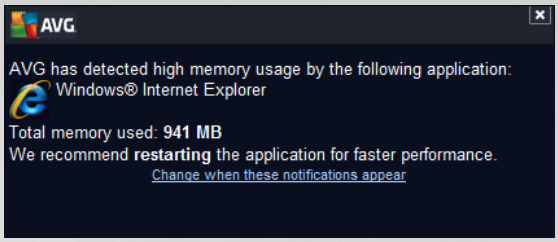
System tray notifications

Within this section you can suppress display of system tray notifications on the status of the **AVG AntiVirus Free Edition 2015** application. By default, the system notifications are allowed to be displayed. It is highly recommended that you keep this configuration! System notifications inform for example on scanning or updating process launch, or on status change of a **AVG AntiVirus Free Edition 2015** component. You should certainly pay attention to these announcement!

However, if for some reason you decide that you do not wish to be informed this way, or that you would like to see only certain notifications *(related to a specific AVG AntiVirus Free Edition 2015 component)* to be displayed, you can define and specify your preferences by checking/unchecking the following options:

- ***Display system tray notifications*** *(on, by default)* - by default, all notifications are displayed. Uncheck this item to completely turn off the display of all system notifications. When turned on, you can further select what specific notifications should be displayed:
    - ***Update notifications*** *(on, by default)* - decide whether information regarding **AVG AntiVirus Free Edition 2015** update process launch, progress, and finalization should be displayed.
    - ***Component change notifications*** *(off, by default)* - decide whether information regarding component's activity/inactivity, or its possible problem should be displayed. When reporting a component's fault status, this option equals to the informative function of the system tray icon reporting a problem in any **AVG AntiVirus Free Edition 2015** component.
    - ***Resident Shield automatic threat removal notifications*** *(on, by default)* - decide whether information regarding file saving, copying, and opening processes should be displayed or suppressed (*this configuration only demonstrates if the Resident Shield Auto-heal option is on*).
    - ***Scanning notifications*** *(on, by default)* - decide whether information upon automatic launch of the scheduled scan, its progress and results should be displayed.
    - ***Email Scanner notifications*** *(on, by default)* - decide whether information upon scanning of all incoming and outgoing email messages should be displayed.
    - ***Statistical notifications*** *(on, by default)* - keep the option checked to allow regular statistical review notification to be displayed in the system tray.
    - ***Boot time improvement notifications*** *(on, by default)* - keep checked if you want to be informed on how your computer boot time has improved after having installed **AVG AntiVirus Free Edition 2015**.

o ***AVG Advisor notifications*** *(on, by default)* - decide whether information upon AVG Advisor activities should be displayed in the slide panel on the system tray.

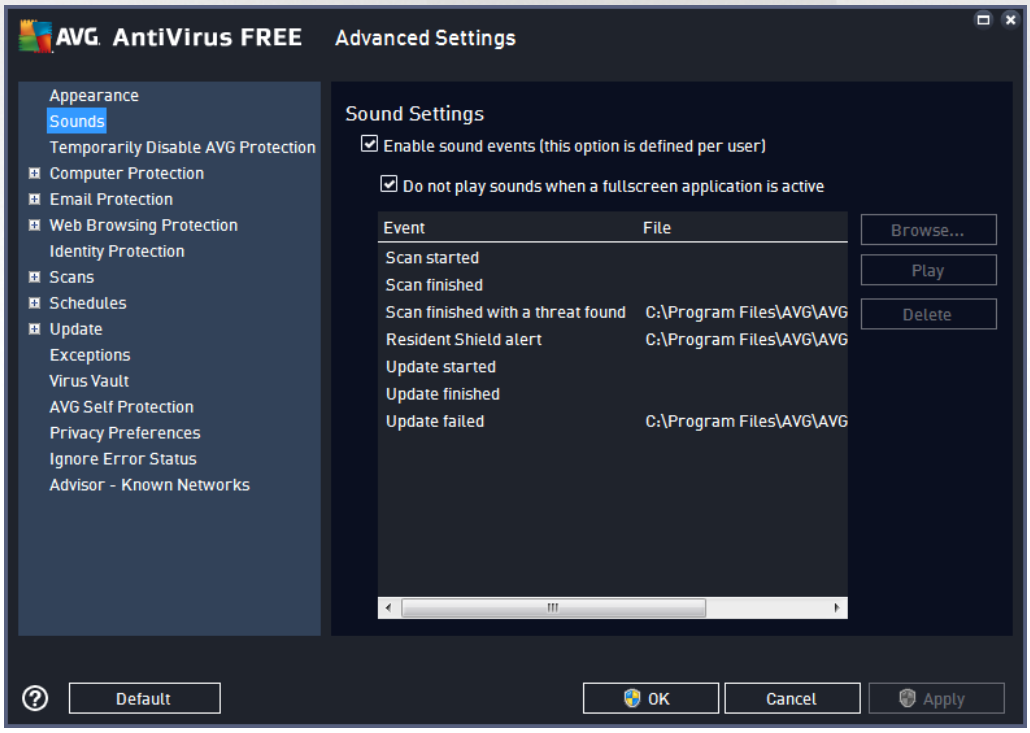

AVG
AVG has detected high memory usage by the following application:
Windows® Internet Explorer
Total memory used: 941 MB
We recommend restarting the application for faster performance.
Change when these notifications appear

Gaming mode

This AVG function is designed for full-screen applications where possible AVG information balloons (*displayed e.g. when a scheduled scan is started*) would be disturbing (*they could minimize the application or corrupt its graphics*). To avoid this situation, keep the checkbox for the ***Enable gaming mode when a full-screen application is executed*** option marked (*default setting*).

9.2. Sounds

Within the ***Sounds*** dialog you can specify whether you want to be informed about specific **AVG AntiVirus Free Edition 2015** actions by a sound notification:



The settings are only valid for the current user account. That means, each user on the computer can have their own sound settings. If you want to allow the sound notification, keep the ***Enable sound events*** option checked (*the option is on, by default*) to activate the list of all relevant actions. Further, you may want to check the ***Do not play sounds when fullscreen application is active*** option to suppress the sound notification in situations

when it might be disturbing *(see also the Gaming mode section of the Advanced settings/Appearance chapter in this document)*.

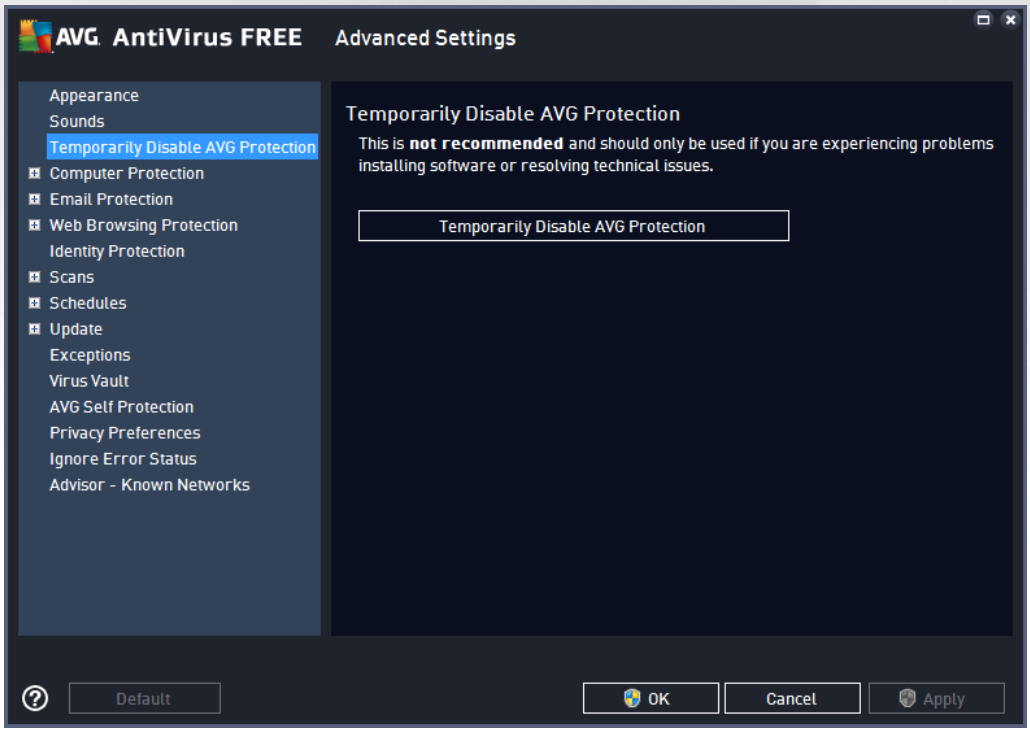
Control buttons

- ***Browse*** - Having selected the respective event from the list, use the ***Browse*** button to search your disk for the desired sound file you want to assign to it. *(Please note that only *.wav sounds are supported at the moment!)*
- ***Play*** - To listen to the selected sound, highlight the event in the list and push the ***Play*** button.
- ***Delete*** - Use the ***Delete*** button to remove the sound assigned to a specific event.

9.3. Temporarily disable AVG protection

In the ***Temporarily disable AVG protection*** dialog you have the option of switching off the entire protection secured by your **AVG AntiVirus Free Edition 2015** at once.

Please remember that you should not use this option unless it is absolutely necessary!



In most cases, it is ***not necessary*** to disable **AVG AntiVirus Free Edition 2015** before installing new software or drivers, not even if the installer or software wizard suggests that running programs and applications be shut down first to make sure there are no unwanted interruptions during the installation process. Should you really experience problem during installation, try to deactivate the resident protection *(in the linked dialog, uncheck the **Enable Resident Shield** item)* first. If you do have to temporarily disable **AVG AntiVirus Free Edition 2015**, you should re-enable it as soon as you're done. If you are connected to the Internet or a network during the time your antivirus software is disabled, your computer is vulnerable to attacks.

How to disable AVG protection

- Mark the ***Temporarily disable AVG protection*** checkbox, and confirm your choice by pressing the ***Apply*** button

- In the newly open ***Temporarily disable AVG protection*** dialog specify for how long you wish to disable your **AVG AntiVirus Free Edition 2015**. By default, the protection will be turned off for 10 minutes which should be sufficient for any common task such as installing new software etc. You can decide for a longer time period, however this option is not recommended if not absolutely necessary. Afterwards, all deactivated components will be automatically activated again. At most, you can disable the AVG protection till the next computer restart.

AVG AntiVirus FREE
Temporarily Disable AVG Protection
Warning:
Disabling AVG protection will leave your computer vulnerable to threats. (You can re-enable AVG protection at any time by right-clicking the AVG tray icon and selecting "Enable AVG protection").
Disable AVG for:
10 minutes
OK
Cancel

9.4. Computer Protection

9.4.1. AntiVirus

AntiVirus together with ***Resident Shield*** protect your computer continuously from all known types of viruses, spyware, and malware in general *(including so-called sleeping and non-active malware, i.e. malware that has been downloaded but not yet activated)*.

In the ***Resident Shield Settings*** dialog you can activate or deactivate the resident protection completely by checking or unchecking the ***Enable Resident Shield*** item (*this option is switched on by default*). In addition you can select which features of the resident protection should be activated:

- ***Ask me before removing threats*** *(on by default)* - Keep the option checked to confirm you want to be asked any time a threat is detected before it is removed to Virus Vault. This choice has no impact on the security level, and it only reflects your preferences.This choice has no impact on the security level, and it only reflects your preferences.

- ***Report potentially unwanted applications and spyware threats*** *(on by default)* - Check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** *(off by default)* - Mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.

- ***Scan files on close*** (*off by default*) - On-close scanning ensures that AVG scans active objects (e.g. applications, documents ...) when they are being opened, and also when they are being closed; this feature helps you protect your computer against some types of sophisticated virus.

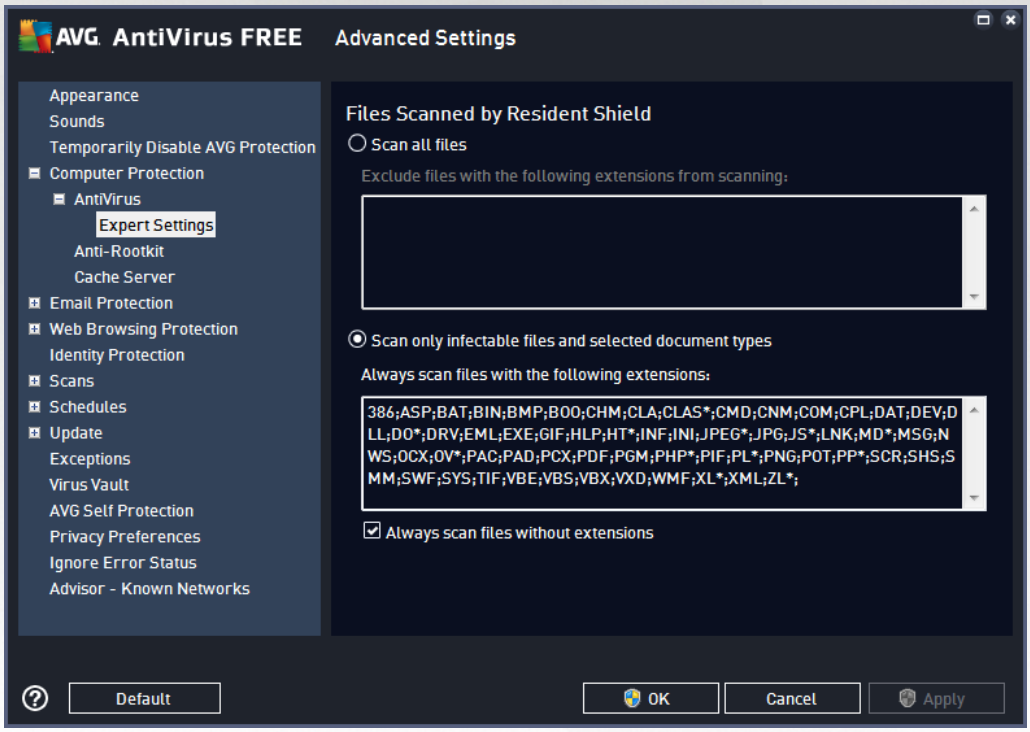
- ***Scan boot sector of removable media*** (*on by default*) - check to scan boot sectors of any inserted USB flash disks, external disk drives and other removable media for threats.

- ***Use heuristics*** (*on by default*) - Heuristic analysis will be used for detection (*dynamic emulation of the scanned object's instructions in a virtual computer environment*).

- ***Scan files referred in registry*** (*on by default*) - This parameter defines that AVG will scan all executable files added to startup registry to avoid a known infection being executed upon next computer startup.

- ***Enable thorough scanning*** (*off by default*) - In specific situations (*in a state of extreme emergency*) you may check this option to activate the most thorough algorithms that will check all possibly threatening objects into the deep. Remember though that this method is rather time consuming.

In the ***Files Sscanned by the Resident Shield*** dialog it is possible to configure which files will be scanned (*by specific extensions*):

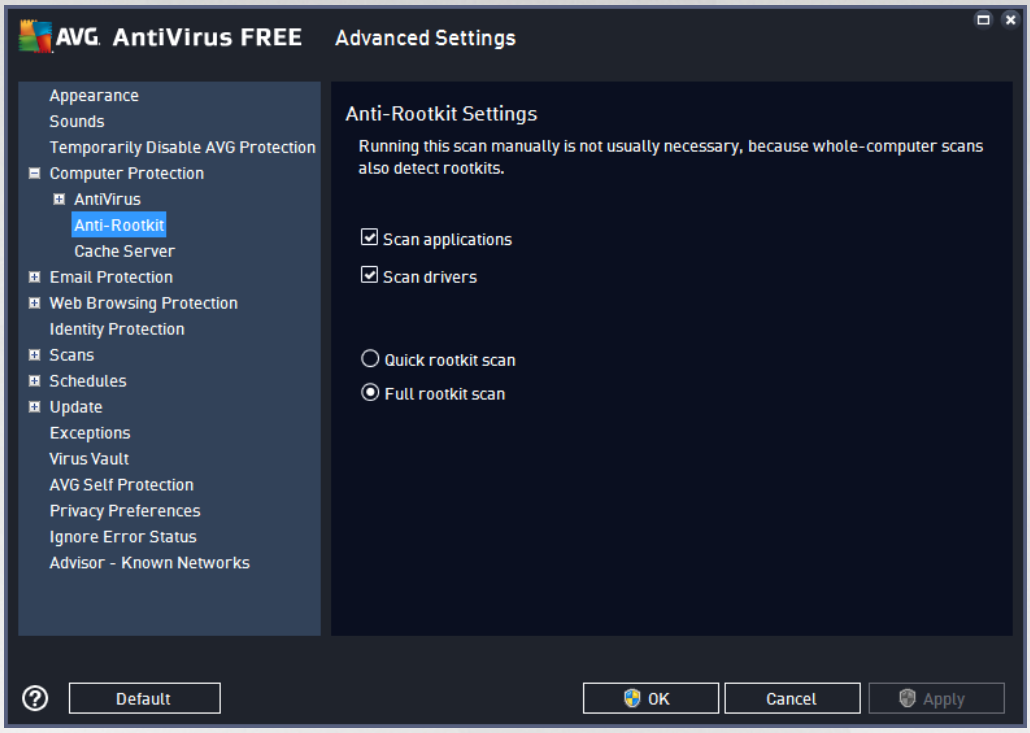


Mark the respective checkbox to decide whether you want to ***Scan all files*** or ***Scan infectable files and selected types of documents*** only. To speed up the scanning and provide the maximum level of protection at the same time, we recommend that you keep the default settings. This way only infectable files will be scanned. In the respective section of the dialog you can also find an editable a list of extensions defining files that are included in scanning.

Check the ***Always scan files without extensions*** (*on by default*) to ensure that even files with no extension and unknown format should be scanned by the Resident Shield. We recommend that you keep this feature switched on, as files without extensions are suspicious.

9.4.2. Anti-Rootkit

In the ***Anti-Rootkit settings*** dialog you can edit the ***Anti-Rootkit*** service configuration and specific parameters of anti-rootkit scanning. The anti-rootkit scanning is a default process included in the Whole Computer Scan:



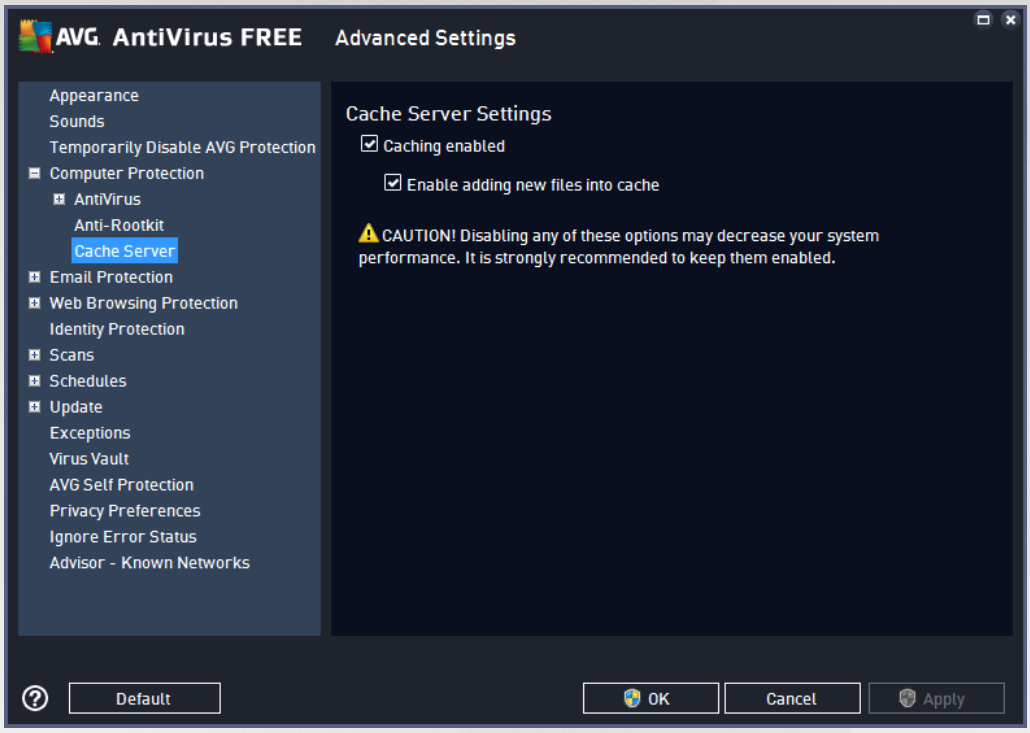
Scan applications and ***Scan drivers*** enable you to specify in detail what should be included in anti-rootkit scanning. These settings are intended for advanced users; we recommend that you keep all options switched on. Further you can pick the rootkit scanning mode:

Further you can pick the rootkit scanning mode:

- ***Quick rootkit scan*** - scans all running processes, loaded drivers and the system folder (*typically c:\Windows*)
- ***Full rootkit scan*** - scans all running processes, loaded drivers, the system folder (*typically c:\Windows*), plus all local disks (*including the flash disk, but excluding floppy disk/CD drives*)

9.4.3. Cache Server

The ***Cache Server Settings*** dialog refers to the cache server process designed to speed up all types of **AVG AntiVirus Free Edition 2015** scans:



It cache server gathers and keeps information of trustworthy files (*a files is considered trustworthy if signed with digital signature of a trustworthy source*). These files are then automatically taken for safe, and do not need to be re-scanned; therefore these files are skipped during scanning.

The ***Cache Server Settings*** dialog offers the following options of configuration:

- ***Caching enabled*** (*on by default*) - uncheck the box to switch off the ***Cache Server***, and empty the cache memory. Please note that scanning might slow down, and overall performance of your computer decrease, as every single file in use will be scanned for viruses and spyware first.
- ***Enable adding new files into cache*** (*on by default*) - uncheck the box to stop adding more files into the cache memory. Any already cached files will be kept and used until caching is turned off completely, or until the next definitions update.

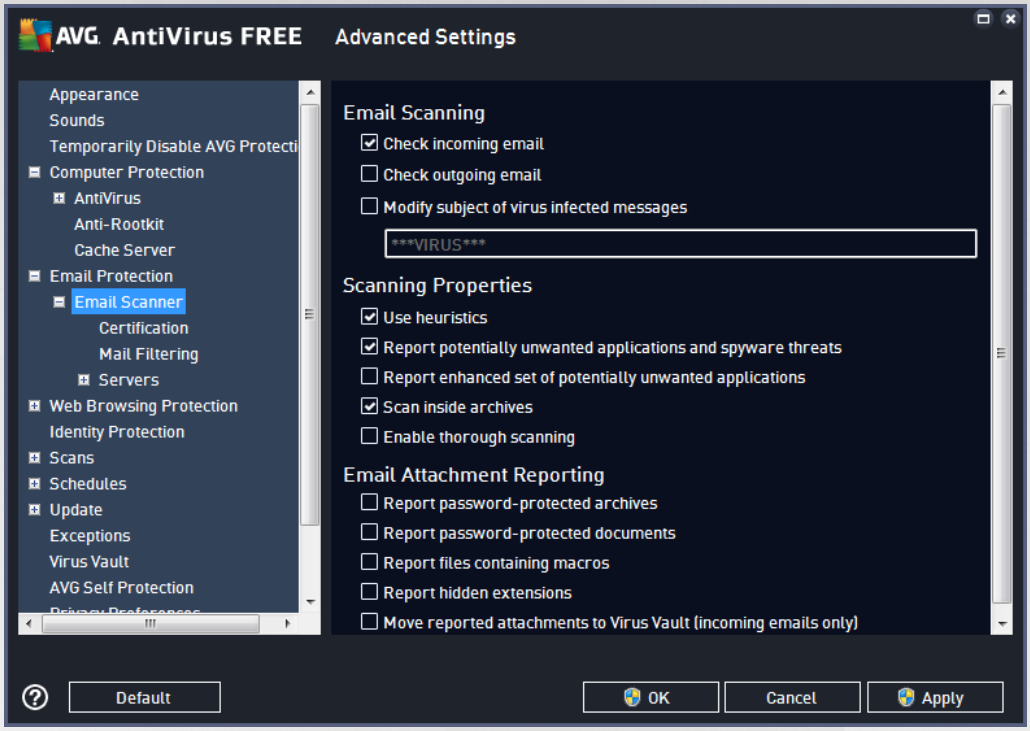
Unless you have a good reason to switch the cache server off, we strongly recommend that you keep the default settings and let both the option on! Otherwise you may experience a significant decrease of your system speed and performance.

9.5. Email Protection

In this section you can edit the detailed configuration of Email Scanner:

9.5.1. Email Protection

The ***Email Scanner*** dialog is divided into three sections:



Email Scanning

In this section, you can set these basics for incoming and/or outgoing email messages:

- ***Check incoming email*** (*on by default*) - mark to switch on/off the option of scanning of all email messages delivered to your email client
- ***Check outgoing email*** (*off by default*) - mark to switch on/off the option of scanning of all emails sent from your account
- ***Modify subject of virus infected messages*** (*off by default*) - if you want to be warned the scanned email message was detected as infectious, mark this item and fill in the desired text into the text field. This text will then be added to the "Subject" field for each detected email message for easier identification and filtering. The default value is ***VIRUS*** which we recommend that you keep.

Scanning Properties

In this section, you can specify how the email messages will be scanned:

- ***Use heuristics*** (*on by default*) - check to use heuristics detection method when scanning email messages. When this option is on, you can filter email attachments not only by extension but also the actual contents of the attachment will be considered. The filtering can be set in the Mail Filtering dialog.

- ***Report potentially unwanted applications and spyware threats*** (*on by default*) - check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** (*off by default*) - mark to detect extended package of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.

- ***Scan inside archives*** (*on by default*) - check to scan contents of archives attached to email messages.

- ***Enable thorough scanning*** (*off by default*) - in specific situations (*e.g. suspicious of your computer being infected by an virus or exploit*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.

Email Attachments Reporting

In this section, you can set additional reports about potentially dangerous or suspicious files. Please note that no warning dialog will be displayed, only a certification text will be added to the end of the email message, and all such reports will be listed in the Email Protection detection dialog:

- ***Report password protected archives*** - archives (*ZIP, RAR etc.*) that are protected by password are not possible to scan for viruses; check the box to report these as potentially dangerous.

- ***Report password protected documents*** - documents protected by password are not possible to scan for viruses; check the box to report these as potentially dangerous.

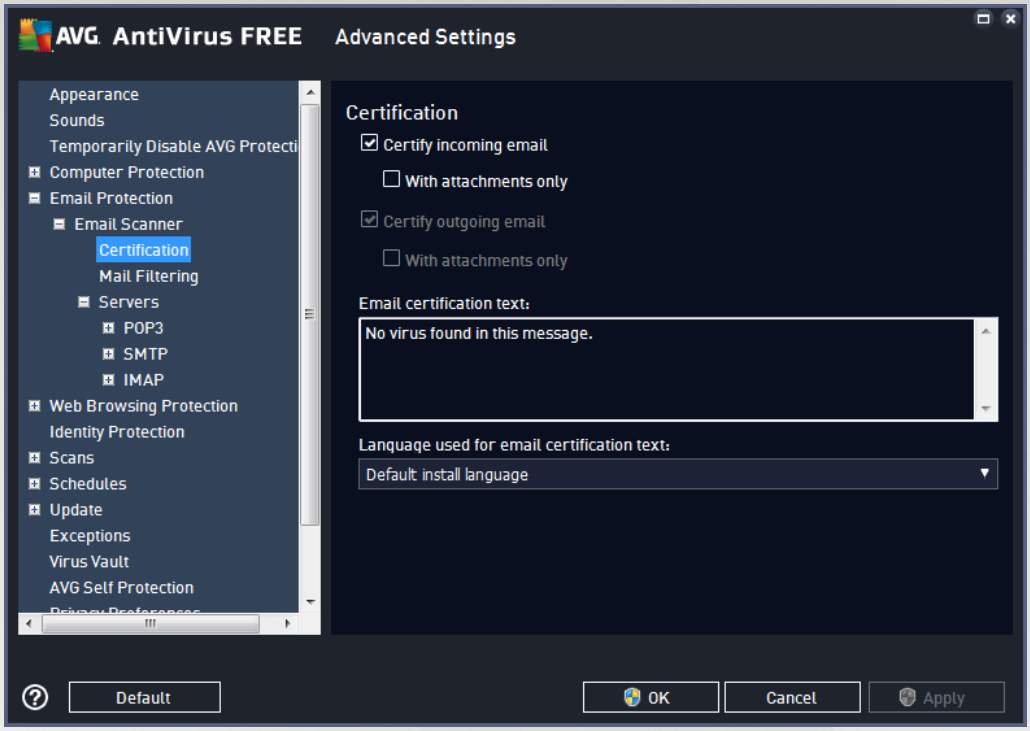
- ***Report files containing macros*** - a macro is a predefined sequence of steps aimed to make certain tasks easier for a user (*MS Word macros are widely known*). As such, a macro can contain potentially dangerous instructions, and you might like to check the box to ensure that files with macros will be reported as suspicious.

- ***Report hidden extensions*** - hidden extension can make e.g. a suspicious executable file "something.txt.exe" appear as harmless plain text file "something.txt"; check the box to report these as potentially dangerous.

- ***Move reported attachments to Virus Vault*** - specify whether you wish to be notified via email about password protected archives, password protected documents, macro containing files and/or files with hidden extension detected as an attachment of the scanned email message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the Virus Vault.

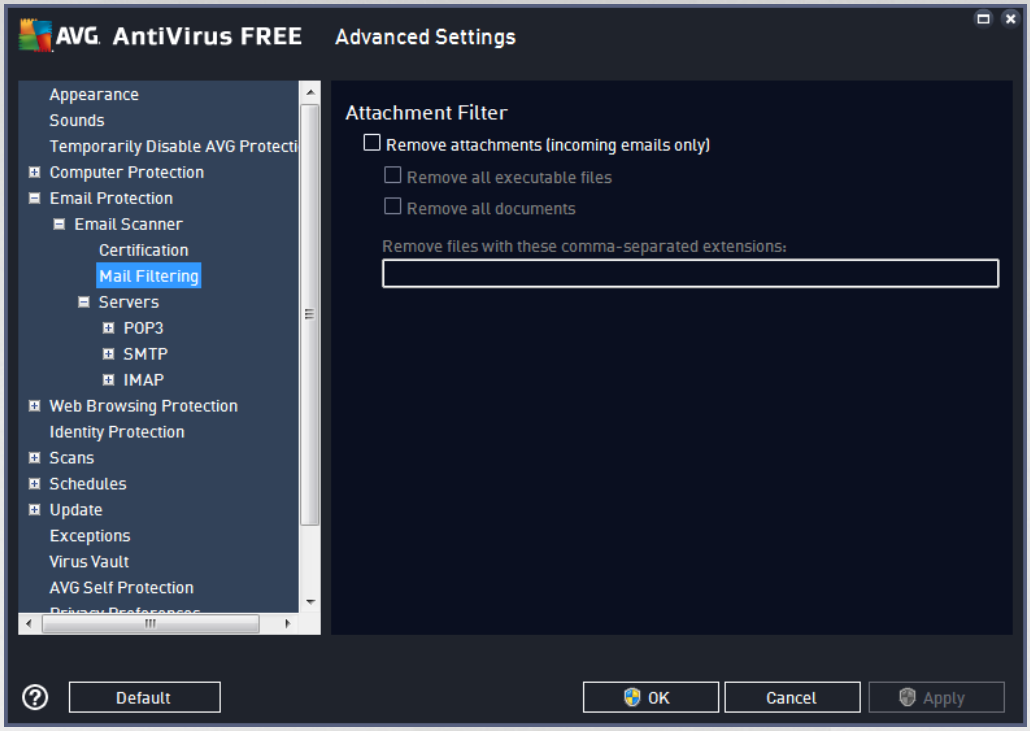
In the ***Certification*** dialog you can mark the specific checkboxes to decide whether you want to certify your incoming mail (***Certify incoming email***) and/or outgoing mail (***Certify outgoing email***). For each of these options you can further specify the ***With attachments only*** parameter so that the certification is only added to

e-mail messages with attachments:



By default, the certification text consists of just a basic information that states *No virus found in this message.* However, this information can be extended or changed according to your needs: write the desired text of certification into the ***Email certification text*** field. In the ***Language used for the email certification text*** section you can further define in which language the automatically generated part of certification (*No virus found in this message*) should be displayed.

Note: *Please mind that only the default text will be displayed in the requested language, and your customized text will not be translated automatically!*



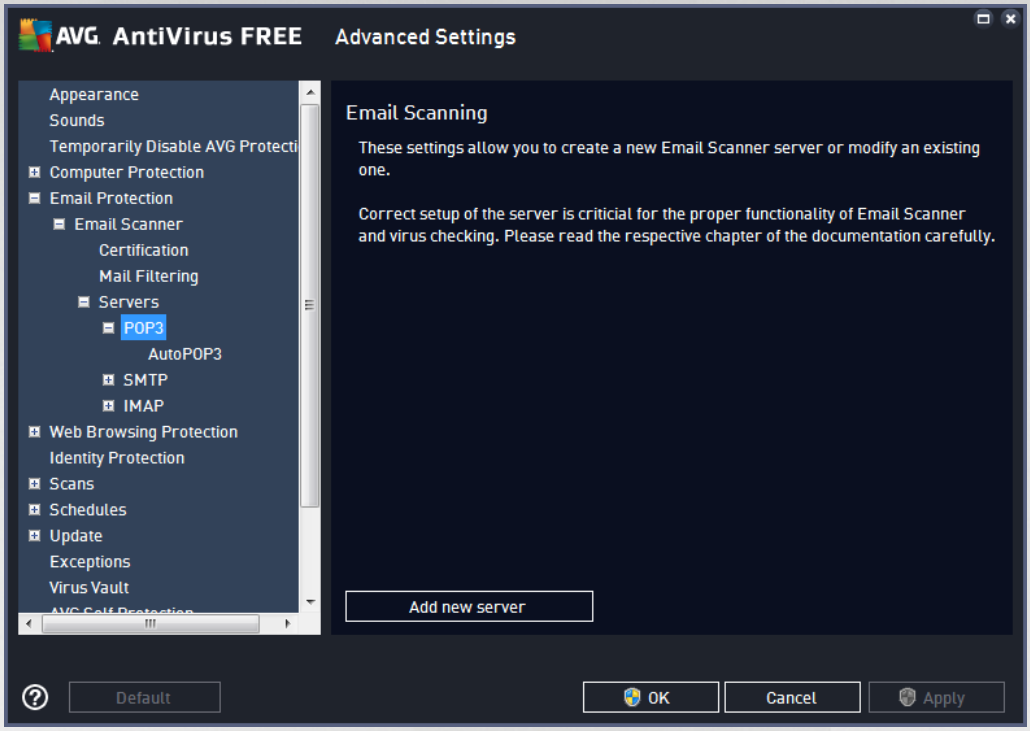
The ***Attachment filter*** dialog allows you to set up parameters for email messages attachment scanning. By default, the ***Remove attachments*** option is switched off. If you decide to activate it, all email message attachments detected as infectious or potentially dangerous will be removed automatically. If you want to define specific types of attachments that should be removed, select the respective option:

- ***Remove all executable files*** - all *.exe files will be deleted
- ***Remove all documents*** - all *.doc, *.docx, *.xls, *.xlsx files will be deleted
- ***Remove files with these comma separated extensions*** - will remove all files with the defined extensions

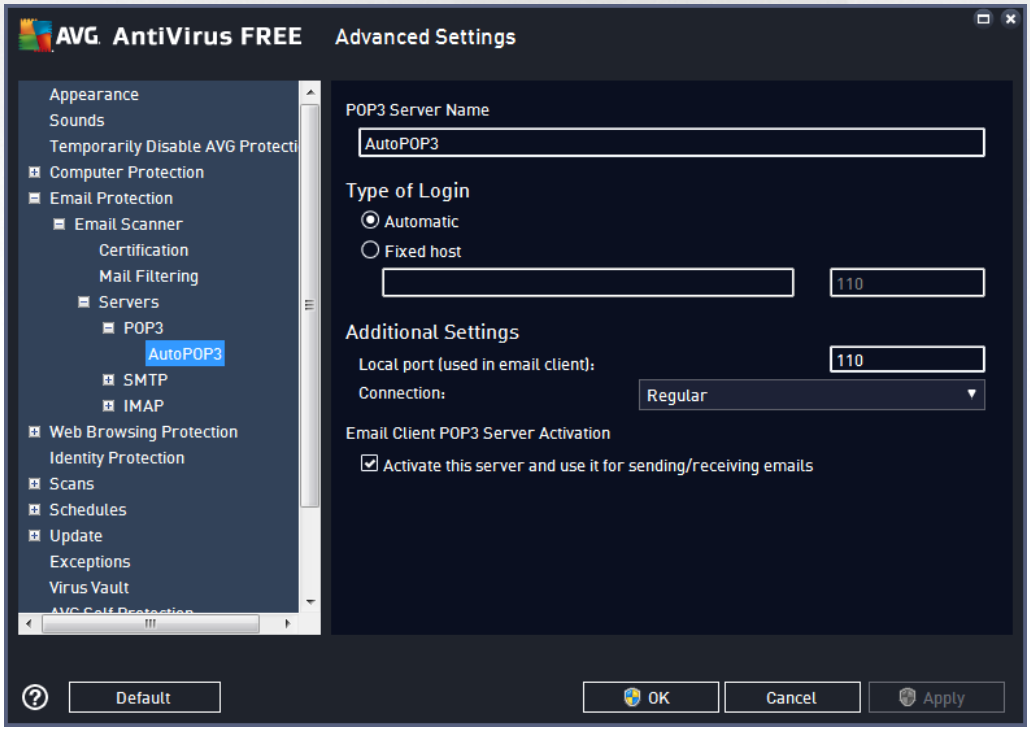
In the ***Servers*** section you can edit parameters of the Email Scanner servers:

- POP3 server
- SMTP server
- IMAP server

You also can define new server for incoming or outgoing mail, using the ***Add new server*** button.

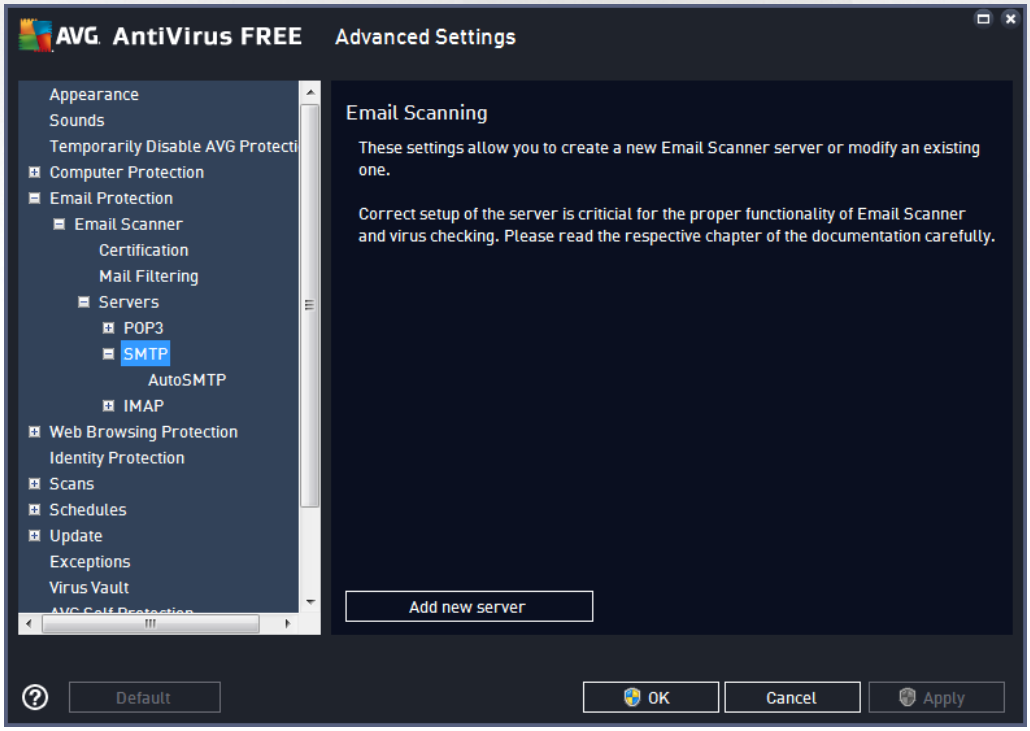


In this dialog you can set up a new Email Scanner server using the POP3 protocol for incoming mail:

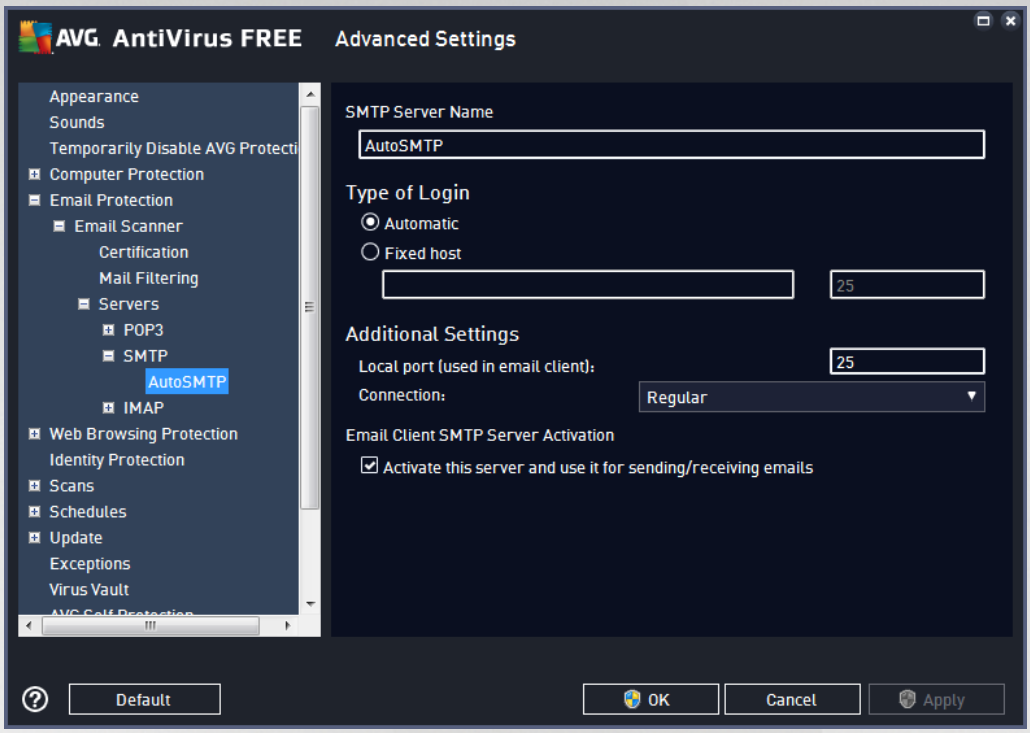


- ***POP3 Server Name*** - in this field you can specify the name of newly added servers (*to add a POP3 server, click the right mouse button over the POP3 item of the left navigation menu*).

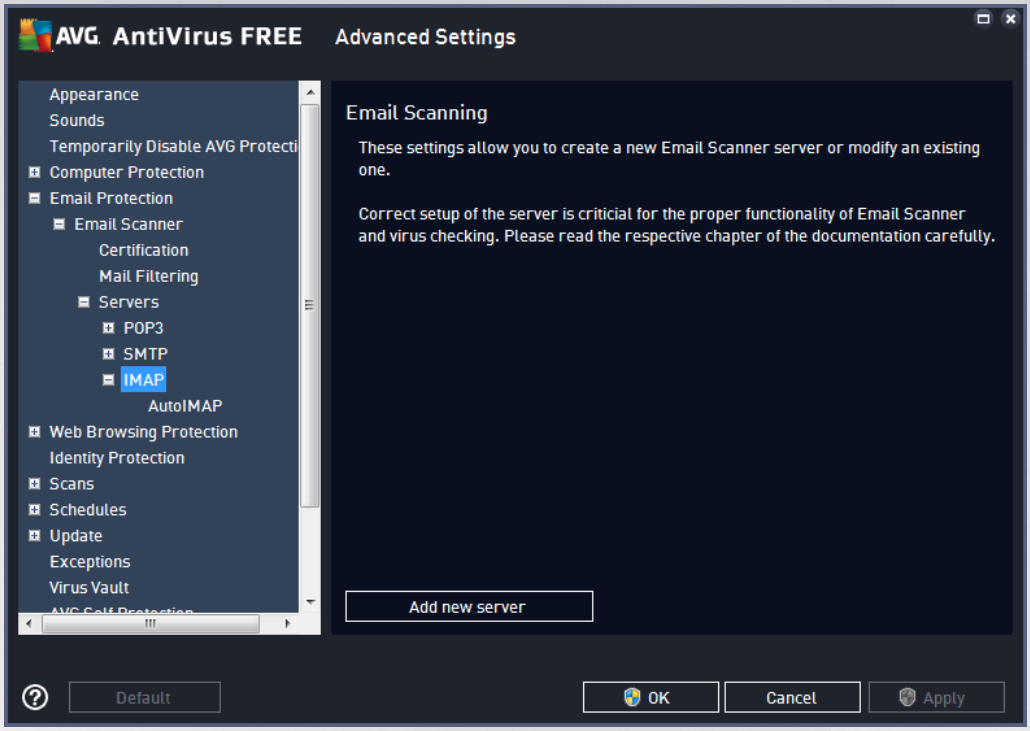
- ***Type of Login*** - defines the method for determining the mail server used for incoming mail:
    - o ***Automatic*** - Login will be carried out automatically, according to your email client settings.
    - o ***Fixed host*** - In this case, the program will always use the server specified here. Please specify the address or name of your mail server. The login name remains unchanged. For a name, you may use a domain name (*for example, pop.acme.com*) as well as an IP address (*for example, 123.45.67.89*). If the mail server uses a non-standard port, you can specify this port after the server name using a colon as the delimiter (*for example, pop.acme.com:8200*). The standard port for POP3 communication is 110.
- ***Additional Settings*** - specifies more detailed parameters:
    - o ***Local port*** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for POP3 communication.
    - o ***Connection*** - in the drop-down menu, you can specify which kind of connection to use: Regular (*standard connection*), SSL (*secured to dedicated port*), or SSL default (*secured to regular port*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
- ***Email Client POP3 Server Activation*** - check/uncheck this item to activate or deactivate the specified POP3 server



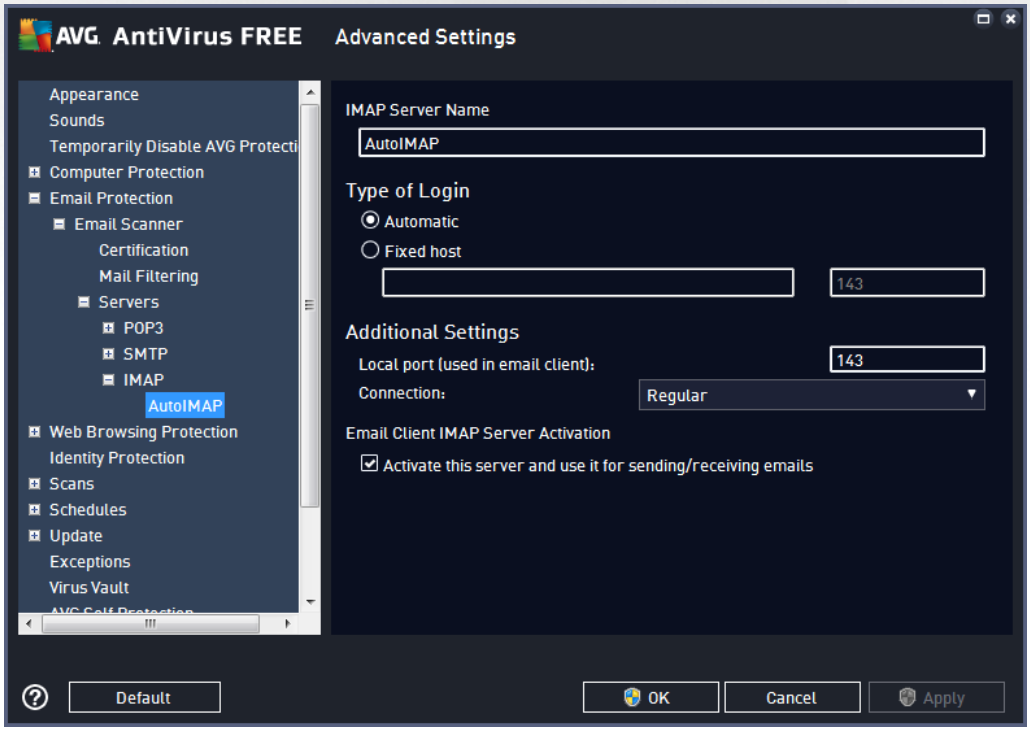
In this dialog you can set up a new Email Scanner server using the SMTP protocol for outgoing mail:



- ***SMTP Server Name*** - in this field you can specify the name of newly added servers (*to add a SMTP server, click the right mouse button over the SMTP item of the left navigation menu*). For automatically created "AutoSMTP" server this field is deactivated.
- ***Type of Login*** - defines the method for determining the mail server used for outgoing mail:
    - o ***Automatic*** - login will be carried out automatically, according to your email client settings
    - o ***Fixed host*** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (*for example, smtp.acme.com*) as well as an IP address (*for example, 123.45.67.89*) for a name. If the mail server uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (*for example, smtp.acme.com:8200*). The standard port for SMTP communication is 25.
- ***Additional Settings*** - specifies more detailed parameters:
    - o ***Local port*** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for SMTP communication.
    - o ***Connection*** - in the drop-down menu, you can specify which kind of connection to use: Regular (*standard connection*), SSL (*secured to dedicated port*), or SSL default (*secured to regular port*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
- ***Email Client SMTP Server Activation*** - check/uncheck this box to activate/deactivate the above specified SMTP server



In this dialog you can set up a new Email Scanner server using the IMAP protocol for outgoing mail:



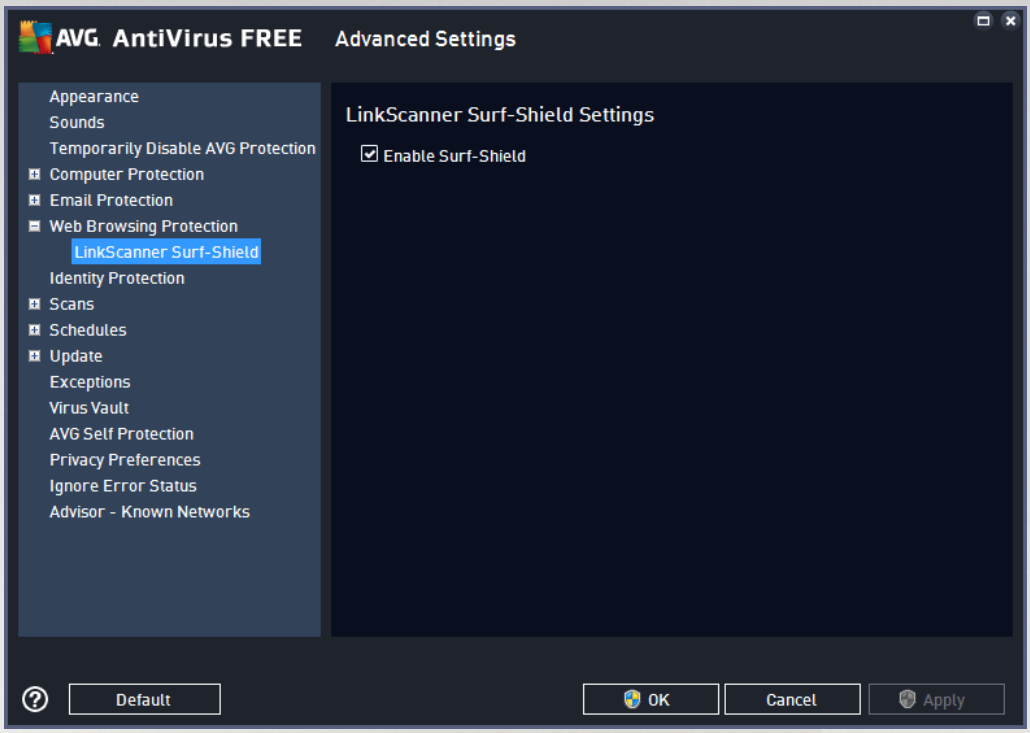
- ***IMAP Server Name*** - in this field you can specify the name of newly added servers (*to add a IMAP server, click the right mouse button over the IMAP item of the left navigation menu*).

- ***Type of Login*** - defines the method for determining the mail server used for outgoing mail:
    - o ***Automatic*** - login will be carried out automatically, according to your email client settings
    - o ***Fixed host*** - in this case, the program will always use the server specified here. Please specify the address or name of your mail server. You may use a domain name (*for example, smtp.acme.com*) as well as an IP address (*for example, 123.45.67.89*) for a name. If the mail server uses a non-standard port, you can type this port behind the server name using a colon as the delimiter (*for example, imap.acme.com:8200*). The standard port for IMAP communication is 143.
- ***Additional Settings*** - specifies more detailed parameters:
    - o ***Local port*** - specifies the port on which the communication from your mail application should be expected. You must then specify in your mail application this port as the port for IMAP communication.
    - o ***Connection*** - in the drop-down menu, you can specify which kind of connection to use: Regular (*standard connection*), SSL (*secured to dedicated port*), or SSL default (*secured to regular port*). If you choose SSL connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
- ***Email Client IMAP Server Activation*** - check/uncheck this box to activate/deactivate the above specified SMTP server

9.6. Web Browsing Protection

9.6.1. LinkScanner Surf-Shield

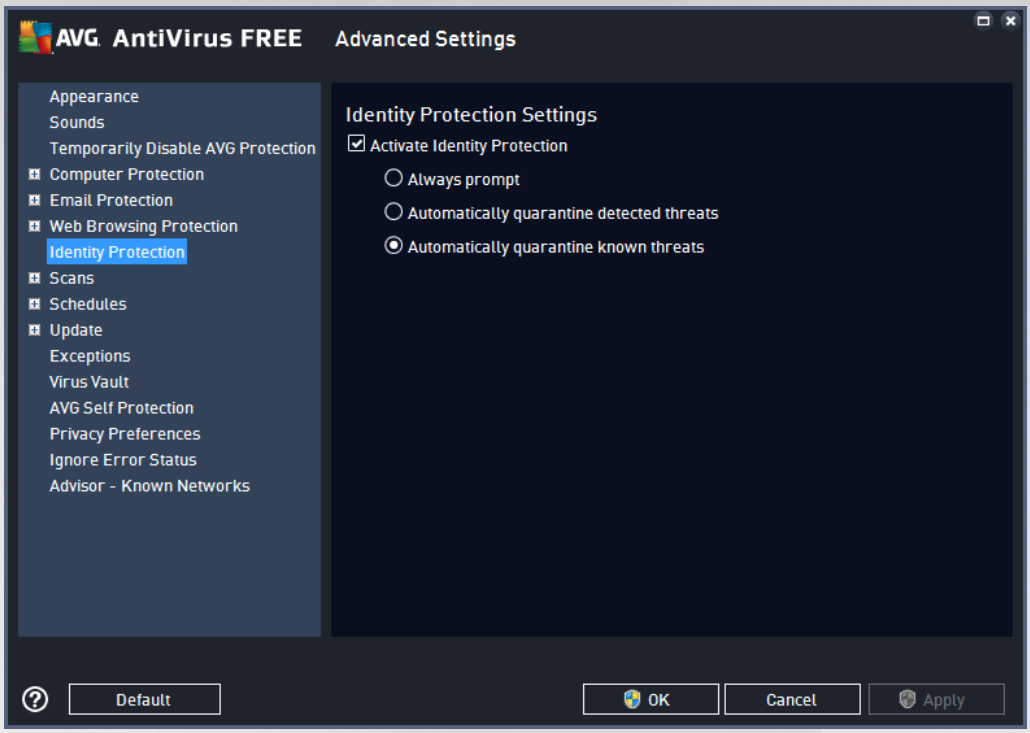
The ***LinkScanner Surf-Shield settings*** dialog allows you to check/uncheck the ***Enable Surf-Shield*** feature (*on by default*) that provides active (*real-time*) protection against exploitive sites as they are accessed. Known malicious site connections and their exploitive content is blocked as they are accessed by the user via a web browser (*or any other application that uses HTTP*).



9.7. Identity Protection

Identity Protection is an anti-malware component that protects you from all kinds of malware (*spyware, bots, identity theft, ...*) using behavioral technologies and provides zero day protection for new viruses *(for a detailed description of the component's functionality please consult the Identity chapter*).

The ***Identity Protection Settings*** dialog allows you to switch the elementary features of the Identity Protection component on/off:



Activate Identity Protection (*on by default*) - uncheck to turn off the Identity component. ***We strongly recommend not doing this unless you have to!*** When the Identity Protection is activated, you can specify what to do when a threat is detected:

- ***Always prompt*** - when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
- ***Automatically quarantine detected threats*** - mark this checkbox to specify that you want to have all possibly detected threats moved to the safe space of the Virus Vault immediately. Keeping the default settings, when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
- ***Automatically quarantine known threats*** (*on by default*) - keep this item marked if you wish all applications detected as possible malware to be automatically and immediately moved to the Virus Vault.

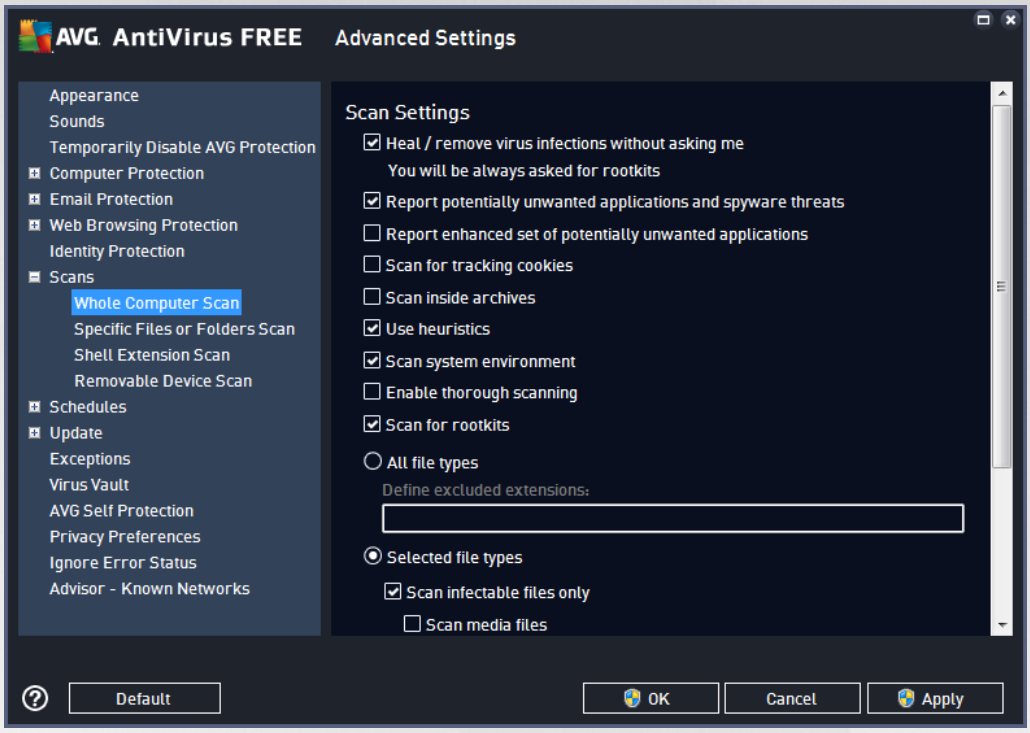
9.8. Scans

The advanced scan settings is divided into four categories referring to specific scan types as defined by the software vendor:

- ***Whole computer scan*** - standard predefined scan of the entire computer
- ***Specific files or folders scan*** - standard predefined scan of selected areas of your computer
- ***Shell extension scan*** - specific scanning of a selected object directly from the Windows Explorer environment
- ***Removable device scan*** - specific scanning of removable devices attached to your computer

9.8.1. Whole computer scan

The ***Whole Computer scan*** option allows you to edit parameters of one of the scans predefined by the software vendor, ***Whole computer scan***:



Scan settings

The ***Scan settings*** section offers a list of scanning parameters that can be optionally switched on/off:

- ***Heal / remove virus infection without asking me*** (*on by default*) - if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.
- ***Report potentially unwanted applications and spyware threats*** (*on by default*) - check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.
- ***Report enhanced set of potentially unwanted applications*** (*off by default*) - mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.
- ***Scan for tracking cookies*** (*off by default*) - this parameter defines that cookies should be detected; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)

- ***Scan inside archives*** (*off by default*) - this parameters defines that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

- ***Use heuristics*** (*on by default*) - heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;

- ***Scan system environment*** (*on by default*) - scanning will also check the system areas of your computer.

- ***Enable thorough scanning*** (*off by default*) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.

- ***Scan for rootkits*** (*on by default*) - Anti-Rootkit scan searches your computer for possible rootkits, i.e. programs and technologies that can cover malware activity in your computer. If a rootkit is detected, this does not necessarily mean your computer is infected. In some cases, specific drivers or sections of regular applications may be misleadingly detected as rootkits.

Further you should decide whether you want to have scanned

- ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated (*having been saved, the commas change into semicolons*) file extensions that should not be scanned.

- ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.

- Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

Adjust how quickly Scan completes

Within the ***Adjust how quickly scan completes*** section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to ***User sensitive*** level, which means that minimum resources are used while you work with your PC, and the scan runs in the high priority mode while you are away.

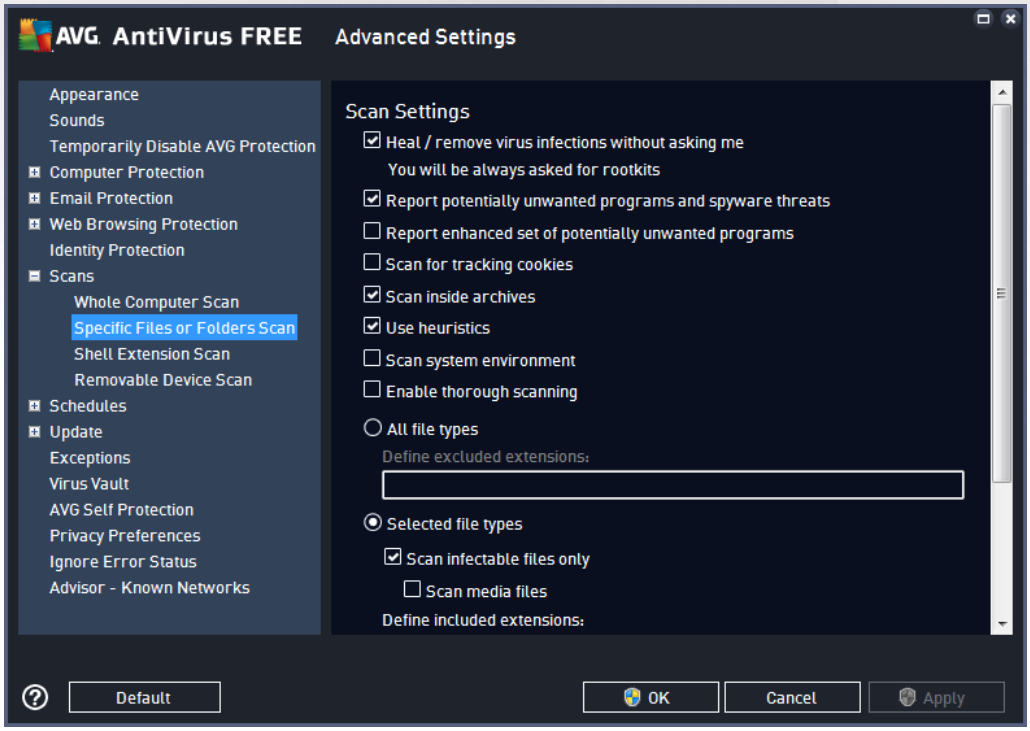
If you want the scanning to run faster, it will take less time but system resources usage will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease system resources usage by extending the scanning duration.

Set additional scan reports ...

Click the ***Set additional scan reports ...*** link to open a standalone dialog window called ***Scan reports*** where you can tick several items to define what scan findings should be reported:

9.8.2. Specific files or folders scan

The editing interface for ***Scan specific files or folders*** is identical to the Whole Computer scan editing dialog. All configuration options are the same; however, the default settings are more strict for the Scan of the whole computer:



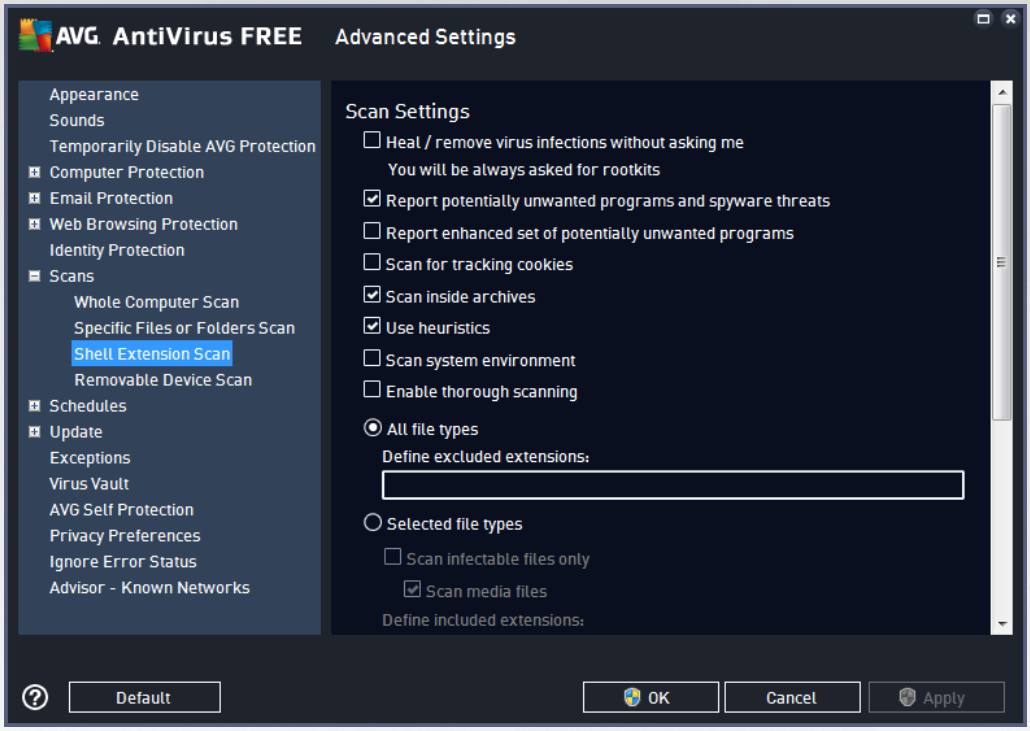
All parameters set up in this configuration dialog apply only to the areas selected for scanning with the Scan of specific files or folders!

Note: *For a description of specific parameters please consult the chapter AVG Advanced Settings / Scans /*

Whole Computer scan.

9.8.3. Shell extension scan

Similar to the previous Whole Computer scan item, this item named ***Shell extension scan*** also offers several options for editing the scan predefined by the software vendor. This time the configuration is related to scanning of specific objects launched directly from the Windows Explorer environment (*shell extension*), see chapter Scanning in Windows Explorer:



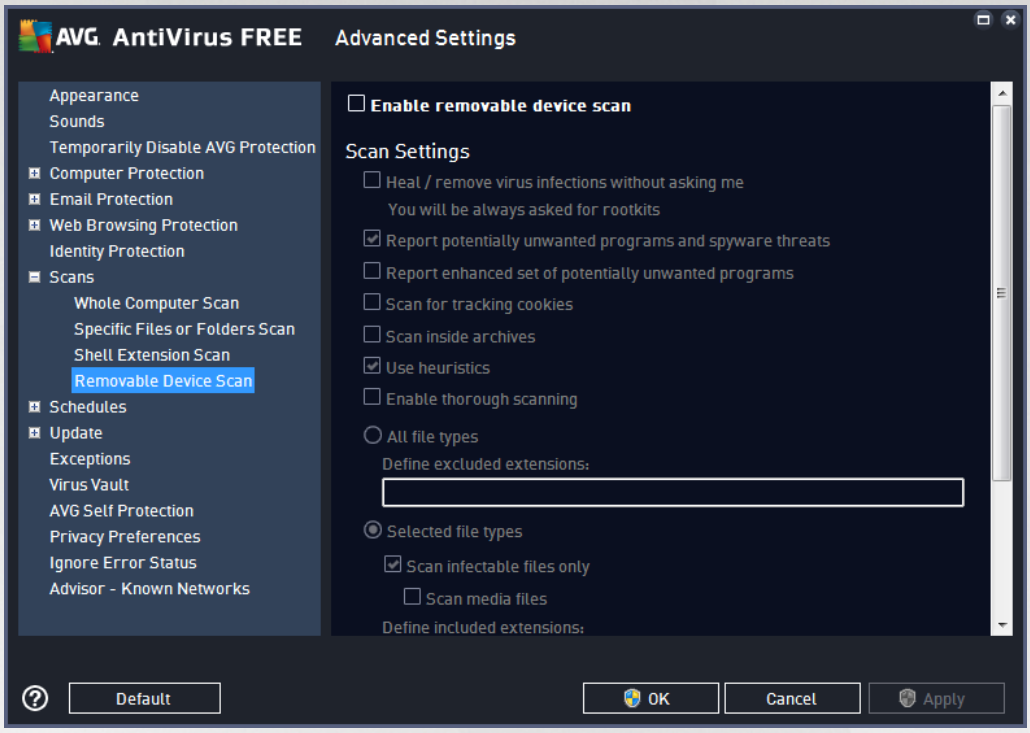
The list of parameters is identical to those available for the Scan of the whole computer. However, the default settings differ (*for instance, Whole Computer scan by default does not check the archives but it does scan the system environment, while with the Shell Extension Scan it is the other way*).

Note: *For a description of specific parameters please consult the chapter AVG Advanced Settings / Scans / Whole Computer scan*.

Compared to Whole Computer scan dialog, the ***Shell extension scan*** dialog also includes the section named ***Other settings related to AVG User Interface***, where you can specify whether you want the scan progress and scan results to be accessible from the AVG user interface. You also can define that the scan result should only be displayed in case an infection is detected during scanning.

9.8.4. Removable device scan

The editing interface for ***Removable device scan*** is also very similar to the Whole Computer scan editing dialog:



The ***Removable device scan*** is launched automatically once you attach any removable device to your computer. By default, this scanning is switched off. However, it is crucial to scan removable devices for potential threats since these are a major source of infection. To have this scanning ready and launched automatically when needed, mark the ***Enable Removable device scan*** option.

Note: *For a description of specific parameters please consult the chapter AVG Advanced Settings / Scans / Whole Computer scan.*

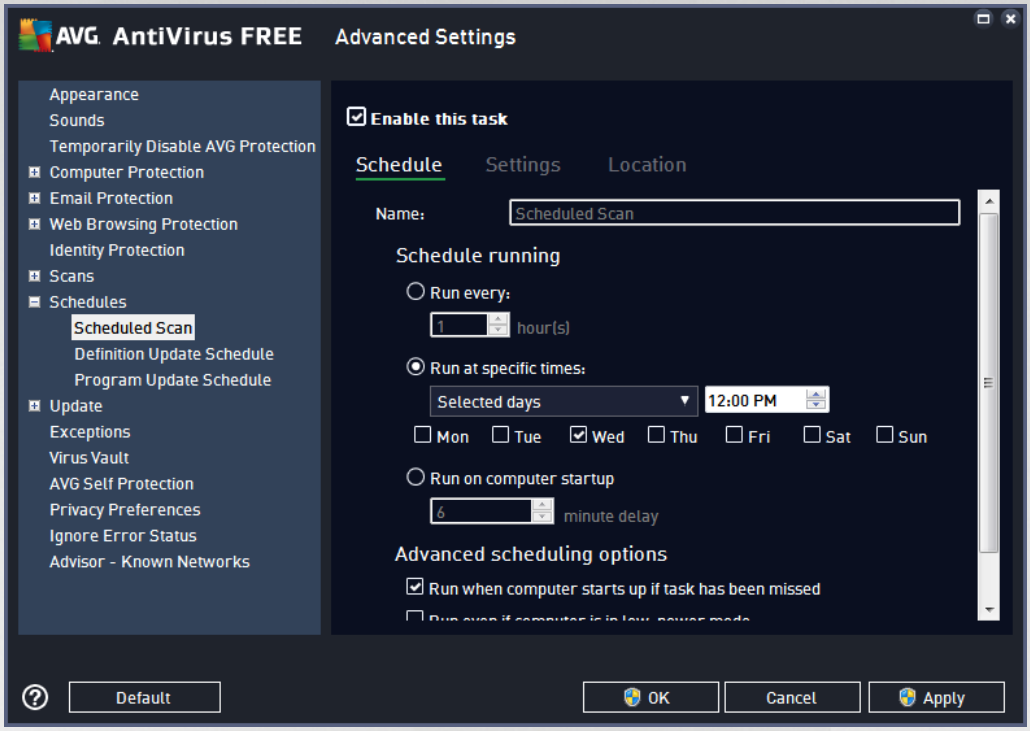
9.9. Schedules

In the ***Schedules*** section you can edit the default settings of:

- Scheduled scan
- Definitions update schedule
- Program update schedule

9.9.1. Scheduled Scan

In this dialog, you can configure settings of a scheduled scan, and set it to run at regular intervals. Parameters of the scheduled scan can be edited on three tabs. On each tab you can first check/uncheck the ***Enable this task*** item to simply deactivate the scheduled test temporarily, and switch it on again as the need arises:



In the text field called ***Name*** (*deactivated for all default schedules*) there is the name assigned to this very schedule by the program vendor. Unfortunately, within **AVG AntiVirus Free Edition 2015** the option of creating new scan schedules is not supported.

AVG AntiVirus Free Edition 2015 is provided free-of-charge, and its functionality is limited. While using AVG AntiVirus Free Edition 2015 you might discover you would like to have access to further and extended functionality of AVG paid products; then please visit AVG website (http://www.avg.com/) for AVG purchase information.

In this dialog you can further define the following parameters of the scan:

Schedule running

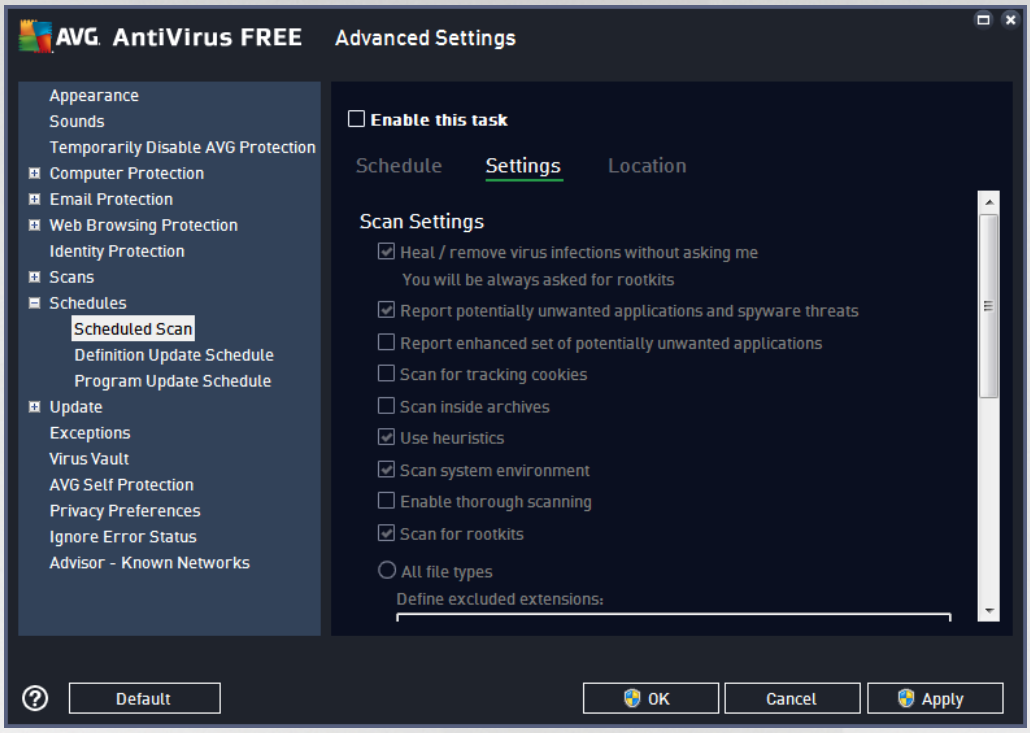
Here, you can specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time (***Run every ...***) or by defining an exact date and time (***Run at specific times***), or possibly by defining an event that the scan launch should be associated with (***Run on computer startup***).

Advanced schedule options

- ***Run on computer startup if task has been missed*** – if you schedule the task to run at a specific time, this option will ensure that the scan will be performed subsequently in case the computer is turned off at the scheduled time.

- ***Run even if computer is in low power mode*** – the task should be performed even if the computer is

running on battery power at the scheduled time.



On the ***Settings*** tab you will find a list of scanning parameters that can be optionally switched on/off. By default, most parameters are switched on and the functionality will be applied during scanning. ***Unless you have a valid reason to change these settings we recommend that you keep the predefined configuration***:

- ***Heal / remove virus infection without asking me*** *(on by default):* if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default):* check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** (*off by default*): mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it can possibly block legal programs, and is therefore switched off by default.

- ***Scan for tracking cookies*** (*off by default*): this parameter defines that cookies should be detected during scanning; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)

- ***Scan inside archives*** (*off by default*): this parameter defines the scanning should check all files even

if they are stored inside an archive, e.g. ZIP, RAR, ...

- ***Use Heuristics*** (*on by default*): heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;

- ***Scan system environment*** (*on by default*): scanning will also check the system areas of your computer;

- ***Enable thorough scanning*** (*off by default*) - in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that can hardly get infected, just to be absolutely sure. Remember though that this method is rather time consuming.

- ***Scan for rootkits*** (*off by default*): tick this item if you want to include the rootkit detection into scanning of the entire computer. The rootkit detection is also available on its own within the Anti-Rootkit component;

Further you should decide whether you want to have scanned

- ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated (*having been saved, the commas change into semicolons*) file extensions that should not be scanned;

- ***Selected file types*** - you can specify that you want to scan only files that are possibly infectable (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus*). Again, you can specify by extensions which files are those that should always be scanned.

- Optionally, you can decide you want to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extension are rather suspicious and should be scanned at all times.

Adjust how quickly Scan completes

Within this section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to ***User sensitive*** level, which means that minimum resources are used while you work with your PC, and the scan runs in the high priority mode while you are away.

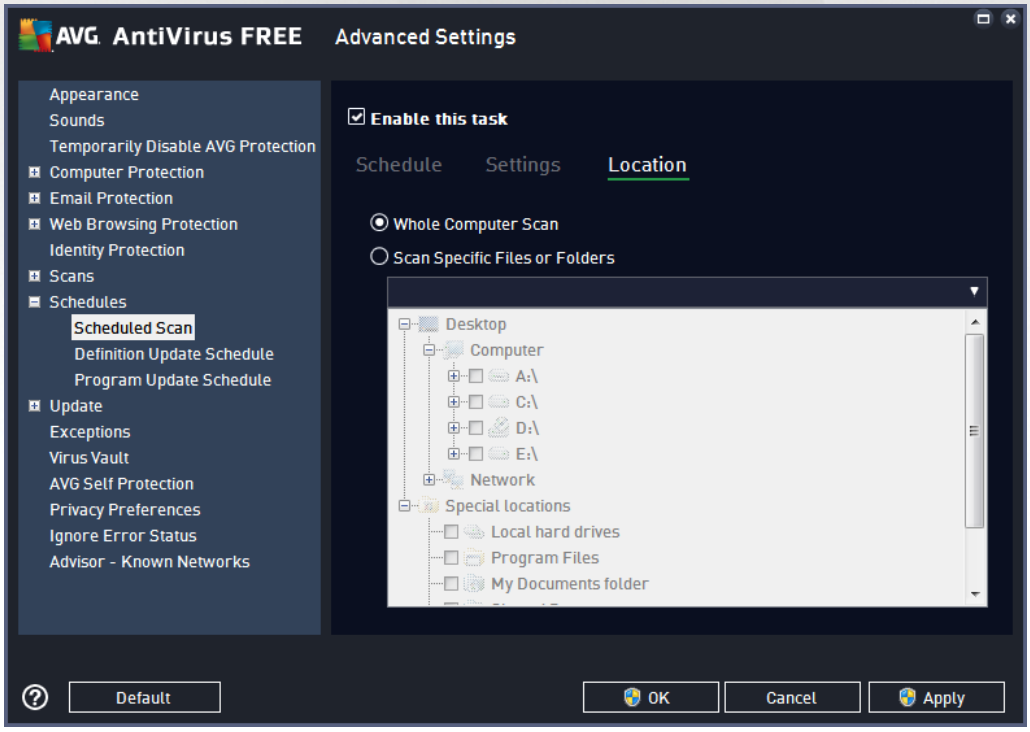
If you want the scanning to run faster, it will take less time but the system resources usage will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease the system resources usage by extending the scanning duration.

Set additional scan reports

Click the ***Set additional scan reports ...*** link to open a standalone dialog window called ***Scan reports*** where you can tick several items to define what scan findings should be reported:

Computer shutdown options

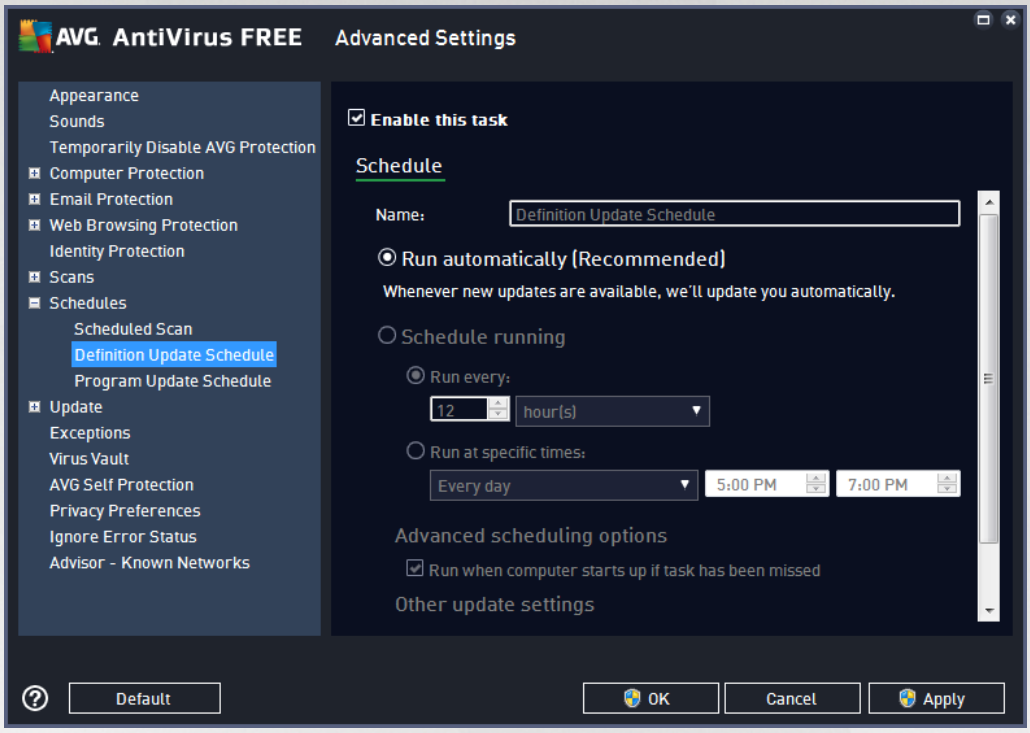
In the ***Computer shutdown options*** section you can decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option activates that allows the computer to shut down even if it is currently locked (***Force shutdown if computer is locked***).



On the ***Location*** tab you can define whether you want to schedule scanning of the whole computer or scanning of specific files or folders. If you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify the folders to be scanned.

9.9.2. Definitions Update Schedule

If really necessary, you can uncheck the ***Enable this task*** item to simply deactivate the scheduled definitions update temporarily, and switch it on again later:



Within this dialog you can set up some detailed parameters of the definitions update schedule. In the text field called ***Name*** (*deactivated for all default schedules*) there is the name assigned to this very schedule by the program vendor.

Schedule running

By default, the task is launched automatically (***Run automatically***) as soon as a new virus definition update is available. Unfortunately, for **AVG AntiVirus Free Edition 2015**, there is no personal settings of this task available. *Should you like to have access to further and extended functionality of AVG paid products; then please visit AVG website (http://www.avg.com/) for AVG purchase information.*

Advanced schedule options

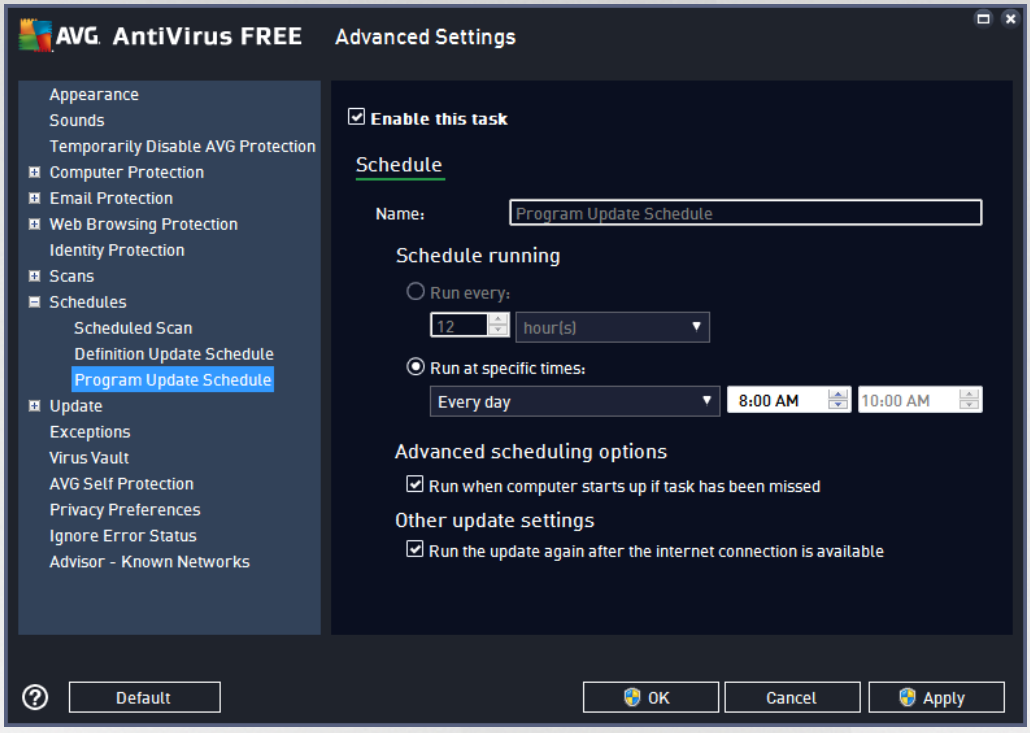
This section allows you to define under which conditions the definitions update should/should not be launched if the computer is in low power mode or switched off completely.

Other update settings

Finally, check the ***Run the update again as soon as the Internet connection is available*** option to make sure than if the Internet connection gets corrupted and the update process fails, it will be launched again immediately after the Internet connection is restored. Once the scheduled update is launched in the time you

have specified, you will be informed on this fact via a pop-up window opened over the AVG system tray icon (*provided that you have kept the default configuration of the the Advanced Settings/Appearance dialog*).

9.9.3. Program Update Schedule



On the ***Schedule settings*** tab you can first check/uncheck the ***Enable this task*** item to simply deactivate the scheduled program update temporarily, and switch it on again as the need arises. In the text field called ***Name*** (*deactivated for all default schedules*) there is the name assigned to this very schedule by the program vendor.

Schedule running

Here, specify the time intervals for the newly scheduled program update launch. The timing can either be defined by the repeated update launch after a certain period of time (***Run every***) or by defining an exact date and time (***Run at specific times***), or possibly by defining an event that the update launch should be associated with (***Run on computer startup***).

Advanced schedule options

This section allows you to define under which conditions the program update should/should not be launched if the computer is in low power mode or switched off completely.

Other update settings

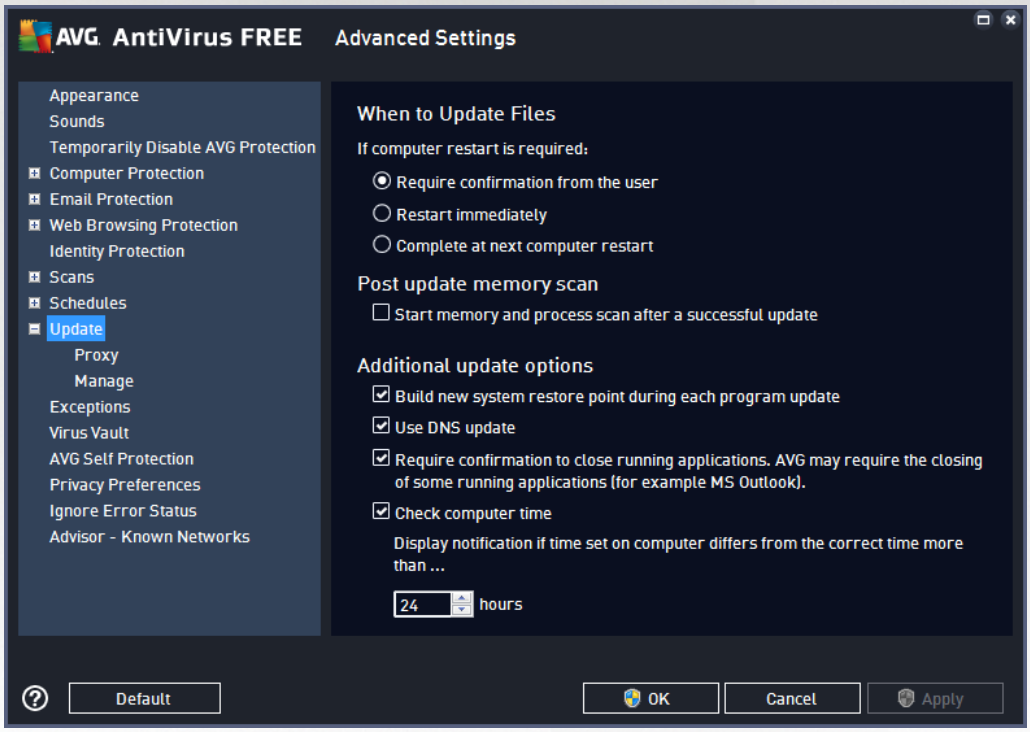
Check the ***Run the update again as soon as the Internet connection is available*** option to make sure than if the Internet connection gets corrupted and the update process fails, it will be launched again immediately after the Internet connection is restored. Once the scheduled update is launched in the time you have

specified, you will be informed on this fact via a pop-up window opened over the AVG system tray icon (*provided that you have kept the default configuration of the the Advanced Settings/Appearance dialog*).

Note: *If a time coincidence of a scheduled program update and scheduled scan occurs, the update process is of higher priority and the scan will get interrupted. In such a case you will be informed about the collision.*

9.10. Update

The ***Update*** navigation item opens a new dialog where you can specify general parameters regarding the AVG update:



When to update files

In this section you can select among three alternative options to be used in case the update process requires your PC restart. The update finalization can be scheduled for the next PC restart, or you can launch the restart immediately:

- ***Require confirmation from the user*** *(by default)* - you will be asked to approve a PC restart needed to finalize the update process
- ***Restart immediately*** - the computer will be restarted automatically immediately after the update process has finished, and your approval will not be required
- ***Complete at next computer restart*** - the update process finalization will be postponed until the next computer restart. Please keep in mind that this option is only recommended if you are sure the computer gets restarted regularly, at least once a day!

Post update memory scan

Mark this checkbox to define you want to launch a new memory scan after each successfully completed update. The latest downloaded update might have contained new virus definitions, and these could be applied in the scanning immediately.

Additional update options

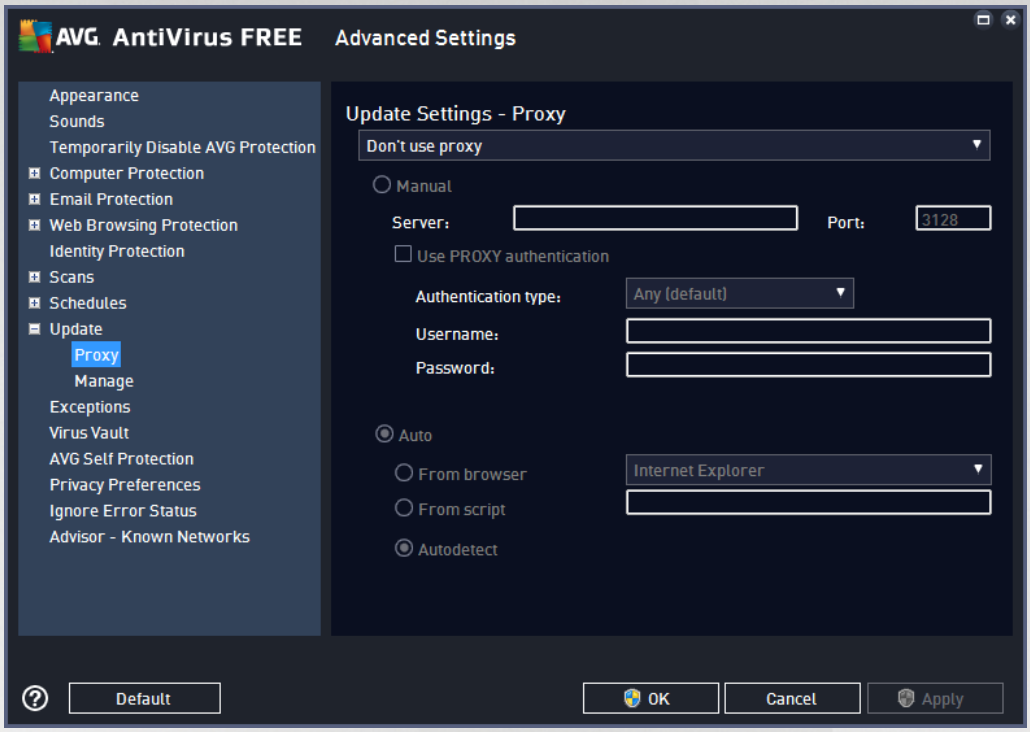
- ***Build new system restore point during each program update*** (*on by default*) - before each AVG program update launch, a system restore point is created. In case the update process fails and your operating system crashes you can always restore your OS in its original configuration from this point. This option is accessible via Start / All Programs / Accessories / System tools / System Restore, but any changes can be recommended to experienced users only! Keep this check-box ticked if you want to make use of this functionality.

- ***Use DNS update*** (*on by default*) - with this item marked, once the update is launched, your **AVG AntiVirus Free Edition 2015** looks up the information about the latest virus database version and the latest program version on the DNS server. Then only the smallest indispensably required update files are downloaded, and applied. This way the total amount of data downloaded is minimized, and the update process runs faster.

- ***Require confirmation to close running applications*** (*on by default*) will help you make sure no currently running applications will be closed without your permission - if required for the update process to be finalized.

- ***Check computer time*** (*on by default*) - mark this option to declare you wish to have notification displayed in case the computer time differs from the correct time more than specified number of hours.

9.10.1. Proxy



The proxy server is a stand-alone server or a service running on a PC that guarantees safer connection to the Internet. According to the specified network rules you can then access the Internet either directly or via the proxy server; both possibilities can also be allowed at the same time. Then, in the first item of the ***Update settings - Proxy*** dialog you have to select from the combo box menu whether you want to:

- ***Don't use proxy*** - default settings
- ***Use proxy***
- ***Try connection using proxy and if it fails, connect directly***

If you select any option using proxy server, you will have to specify some further data. The server settings can be configured either manually or automatically.

Manual configuration

If you select manual configuration (check *the **Manual** option to activate the respective dialog section*) you have to specify the following items:

- ***Server*** - specify the server's IP address or the name of the server
- ***Port*** - specify the number of the port that enables Internet access (*by default, this number is set to 3128 but can be set differently - if you are not sure, contact your network administrator*)

The proxy server can also have configured specific rules for each user. If your proxy server is set up this way, check the ***Use PROXY authentication*** option to verify that your user name and password are valid for

connecting to the Internet via the proxy server.

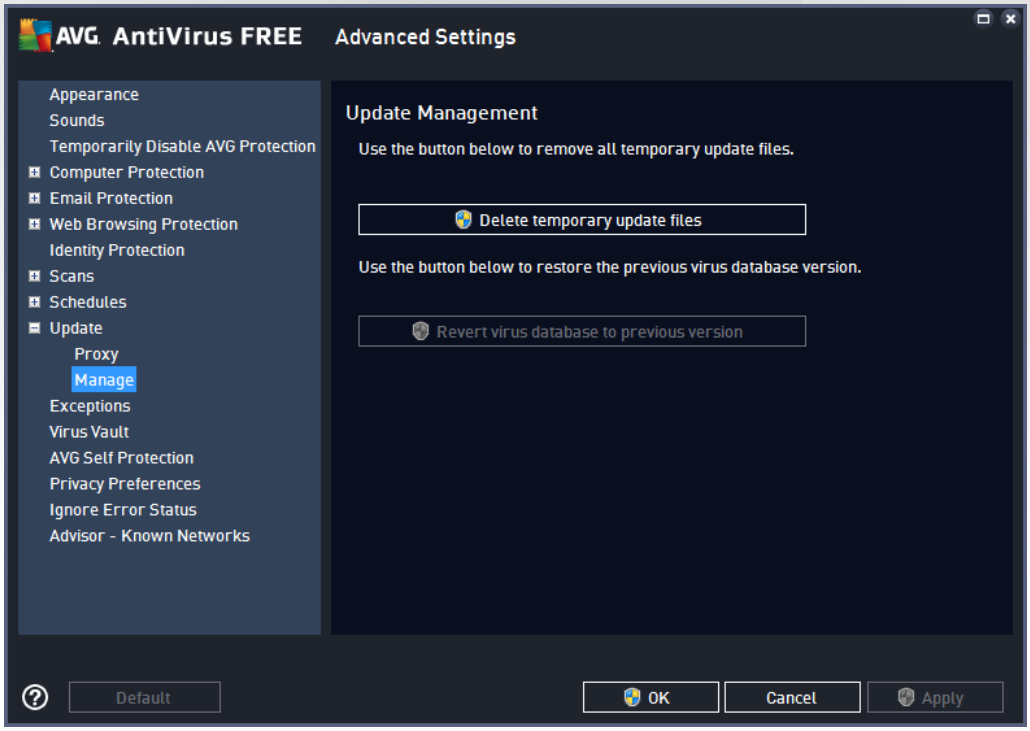
Automatic configuration

If you select automatic configuration (*mark the **Auto** option to activate the respective dialog section*) then please select where the proxy configuration should be taken from:

- ***From browser*** - the configuration will be read from your default Internet browser
- ***From script*** - the configuration will be read from a downloaded script with the function returning the proxy address
- ***Autodetect*** - the configuration will be detected automatically directly from the proxy server

9.10.2. Manage

The ***Update management*** dialog offers two options accessible via two buttons:

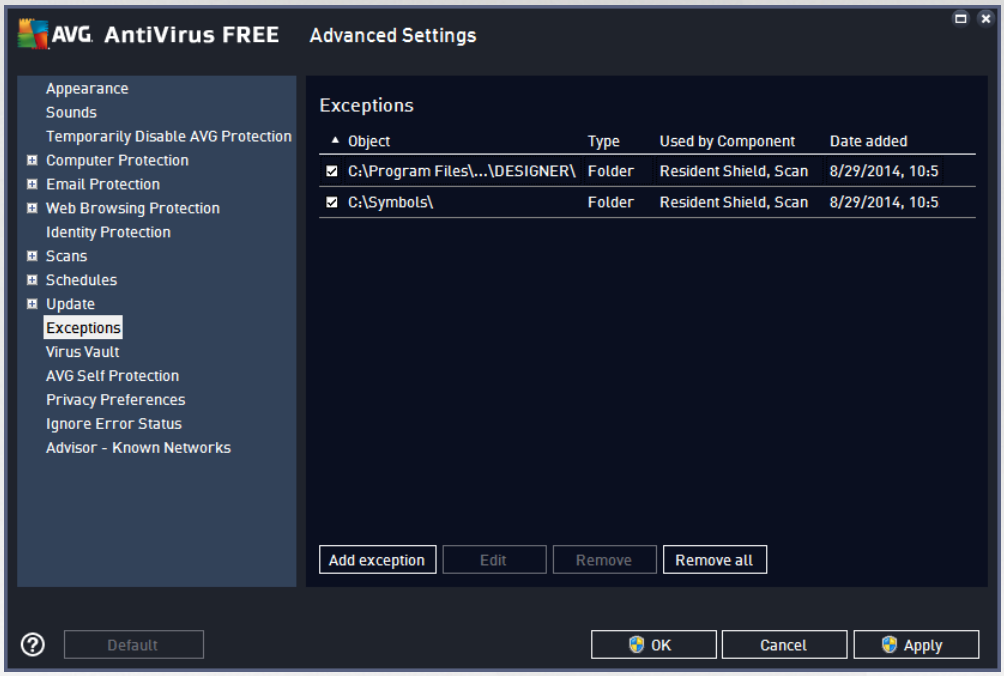


- ***Delete temporary update files*** - press this button to delete all redundant update files from your hard disk (*by default, these files are being saved for 30 days*)
- ***Revert virus database to previous version*** - press this button to delete the latest virus base version from your hard disk, and to return to the previously saved version (*new virus base version will be a part of the following update*)

9.11. Exceptions

In the ***Exceptions*** dialog you can define exceptions, i.e. items that **AVG AntiVirus Free Edition 2015** will ignore. Typically, you will need to define an exception if AVG keeps detecting a program or file as a threat, or blocking a safe website as dangerous. Add such file or website to this exception list, and AVG will not report or block it any more.

Please always make sure that the file, program or website in question really is absolutely safe!



The chart in the dialog displays a list of exceptions, if any have been already defined. Each item has a checkbox next to it. If the checkbox is marked, then the exception is in effect; if not, then the exception is just defined but not currently used. By clicking a column header, you can sort the allowed items according to the respective criteria.

Control buttons

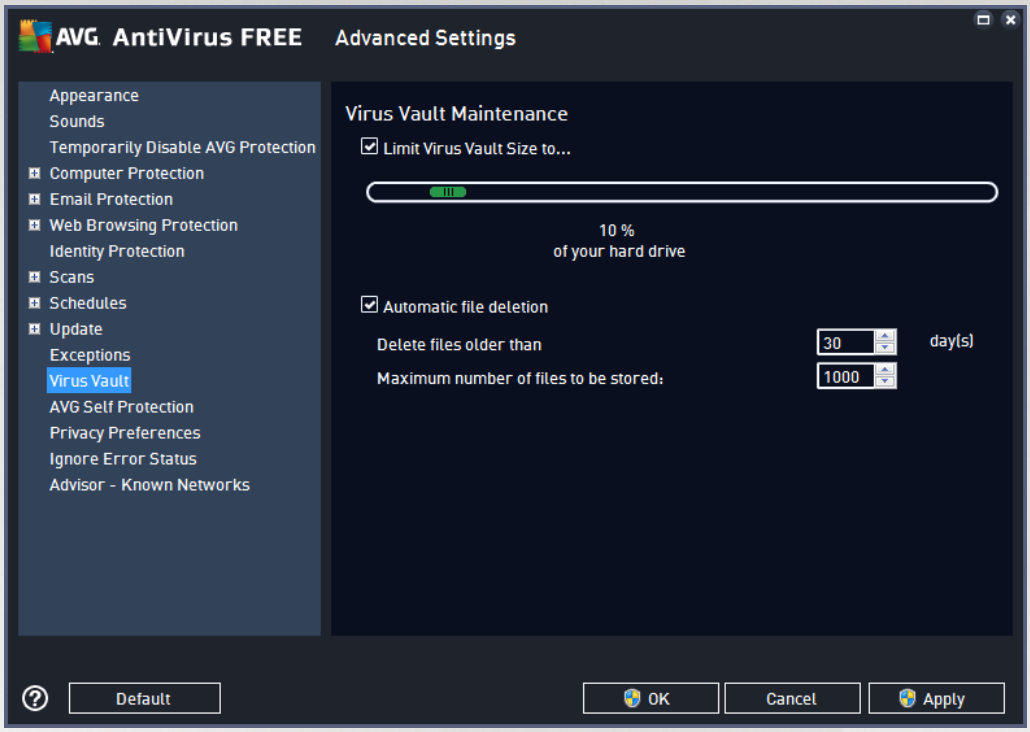
- ***Add exception*** - Click to open a new dialog where you can specify the item that should be excluded from AVG scanning. First, you will be invited to define the type of the object, i.e. whether it is a file, a folder, or URL. Then you will have to browse your disk to provide the path to the respective object, or type the URL. Finally, you can select what AVG features should ignore the selected object *(Resident Shield, Identity Protection, Scan)*.

- ***Edit*** - This button is only active if some exceptions have been already defined, and are listed in the chart. Then, you can use the button to open the editing dialog over a selected exception, and configure the parameters of the exception.

- ***Remove*** - Use this button to cancel a previously defined exception. You can either remove them one by one, or highlight a block of exceptions in the list and cancel the defined exceptions. Having canceled the exception, the respective file, folder or URL will be checked by AVG again. Please note that only the exception will be removed, not the file or folder itself!

- ***Remove all*** - Use this button to delete all defined exceptions in the list.

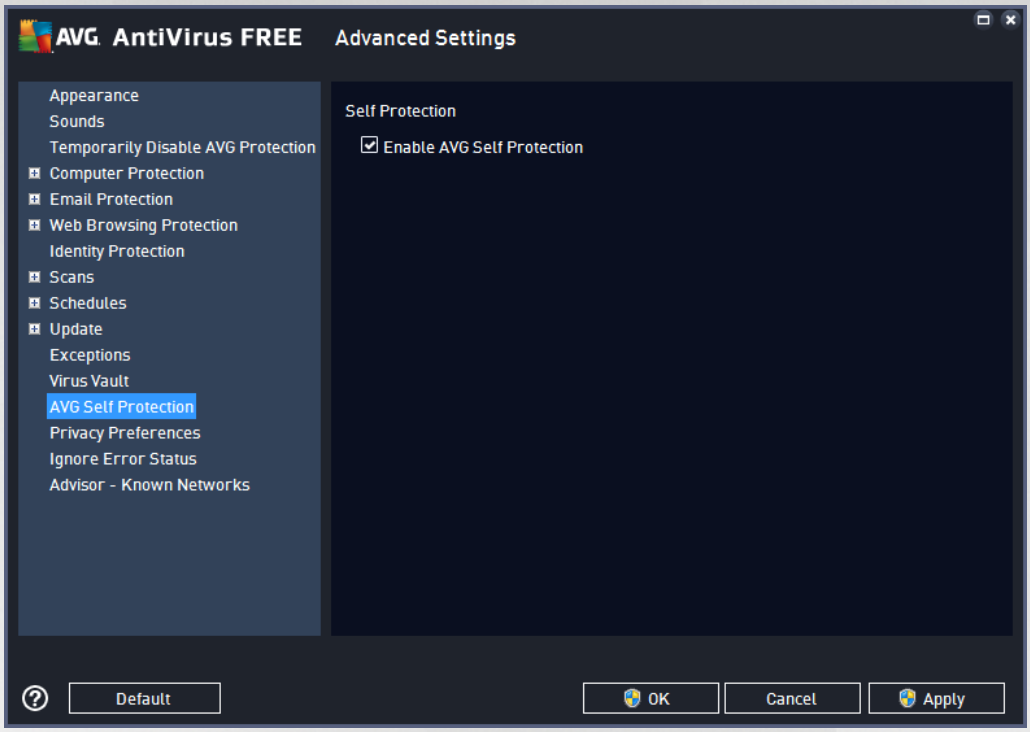
9.12. Virus Vault



The ***Virus Vault maintenance*** dialog allows you to define several parameters regarding the administration of objects stored in the Virus Vault:

- ***Limit Virus Vault size*** - Use the slider to set up the maximum size of the Virus Vault. The size is specified proportionally compared to the size of your local disk.
- ***Automatic file deletion*** - In this section define the maximum length of time that objects should be stored in the Virus Vault (***Delete files older than ... days***), and the maximum number of files to be stored in the Virus Vault (***Maximum number of files to be stored***).

9.13. AVG Self Protection



The ***AVG Self Protection*** enables **AVG AntiVirus Free Edition 2015** to protect its own processes, files, registry keys and drivers from being changed or deactivated. The main reason for this kind of protection is that some sophisticated threats try to disarm the antivirus protection, and then freely cause damage to your computer.

We recommend keeping this feature turned on!

9.14. Privacy Preferences

The ***Privacy Preferences*** dialog invites you to participate in AVG product improvement, and to help us increase the overall Internet security level. Your reporting helps us collect up-to-date information on the latest threats from all participants worldwide, and in return we can improve protection for everyone. The reporting is made automatically, and therefore does not cause you any inconvenience. No personal data is included in the reports. The reporting of detected threats is optional, however, we do ask you to keep this option switched on. It helps us improve protection for both you and other AVG users.

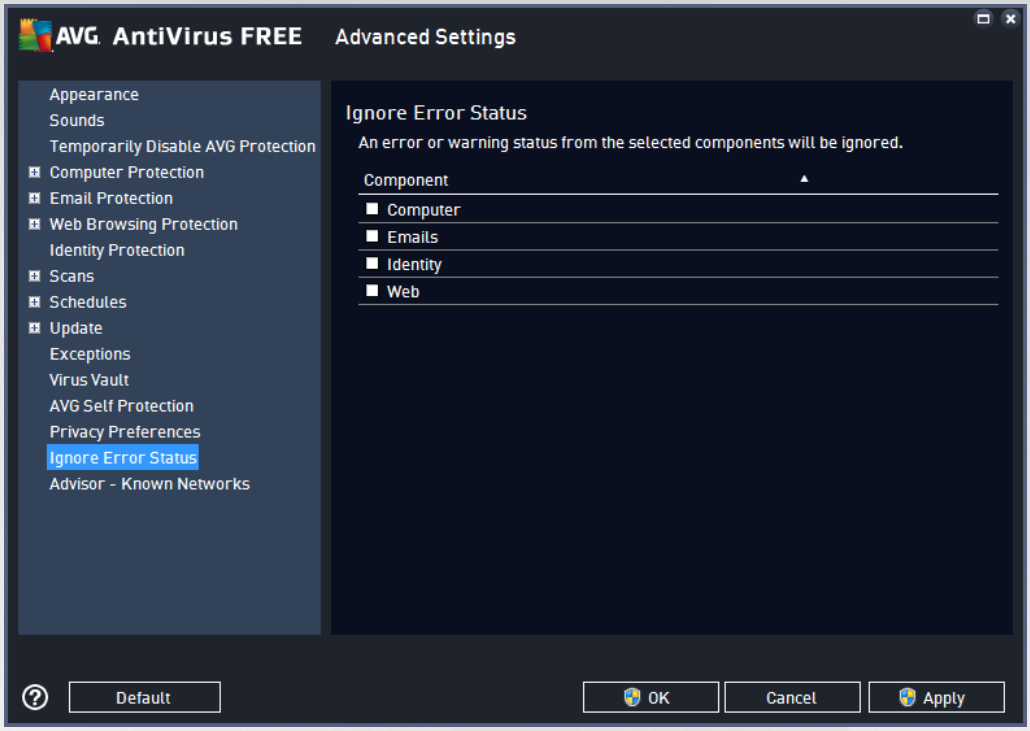
AVG AntiVirus FREE
Advanced Settings
Appearance
Sounds
Temporarily Disable AVG Protection
Computer Protection
Email Protection
Web Browsing Protection
Identity Protection
Scans
Schedules
Update
Exceptions
Virus Vault
AVG Self Protection
Privacy Preferences
Ignore Error Status
Advisor - Known Networks
Privacy Preferences
With your permission, this software can collect anonymous data in accordance with AVG's Privacy Policy. This is used to improve your security and personalize your experience. AVG does not store any personally identifiable information and does not share any information with 3rd parties.
I'd like to help AVG improve its products by participating in AVG's Product Improvement Program.
Send anonymous data about identified or suspicious threats.
Send anonymous data about this software's usage.
Allow in-the-cloud verification of threat detections.
CAUTION: Disabling this feature could impact AVG's ability to protect you correctly. It is strongly recommended to keep this feature enabled.
I'd like AVG to personalize my experience by turning on AVG Personalization
Default
OK
Cancel
Apply

Within the dialog, the following setting options are available:

- ***I'd like to help AVG improve their products by participating in the AVG Product Improvement Program*** *(off by default)* - If you want to help us further improve **AVG AntiVirus Free Edition 2015**, keep the checkbox marked. This will enable all encountered threats to be reported to AVG, so we will be able to collect up-to-date information on malware from all participants worldwide, and in return improve protection for everyone. The report is made automatically, and therefore does not cause you any inconvenience, and no personal data is included in the reports.
    - ***Allow to send anonymous data about identified or suspicious threats*** *(off by default)* - send information about any suspicious or positively dangerous code or behaviour pattern *(can be a virus, spyware, or malicious webpage your are trying to access)* detected on your computer.
    - ***Allow to send anonymous data about product usage*** *(off by default)* - send basic statistics about the application usage, such as number of detections, scans launched, successful or unsuccessful updates etc.
- ***Allow in the cloud verification of detections*** *(on by default)* - detected threats will be checked if really infected, to sort out false positives.
- ***I'd like AVG to personalize my experience by turning on AVG Personalization*** *(off by default)* - this feature anonymously analyzes behavior of programs and applications installed on your PC. Based on this analysis AVG can offer you services targeted directly to your needs, to secure your maximum safety.

9.15. Ignore Error Status

In the ***Ignore error status*** dialog you can tick those components that you do not want to get informed about:



By default, no component is selected in this list. It means that if any component get to an error status, you will be informed about it immediately via:

- system tray icon - while all parts of AVG are working properly, the icon is displayed in four colors; however, if an error occurs, the icon appears with a yellow exclamation mark,
- text description of the existing problem in the Security Status Info section of the AVG main window

There might be a situation that for some reason you need to switch a component off temporarily. ***This is not recommended, you should try to keep all components permanently on and in default configuration***, but it may happen. In this case the system tray icon automatically reports the component's error status. However, in this very case we cannot talk about an actual error since you have deliberately induced it yourself, and you are aware of the potential risk. At the same time, once being displayed in grey color, the icon cannot actually report any possible further error that might appear.

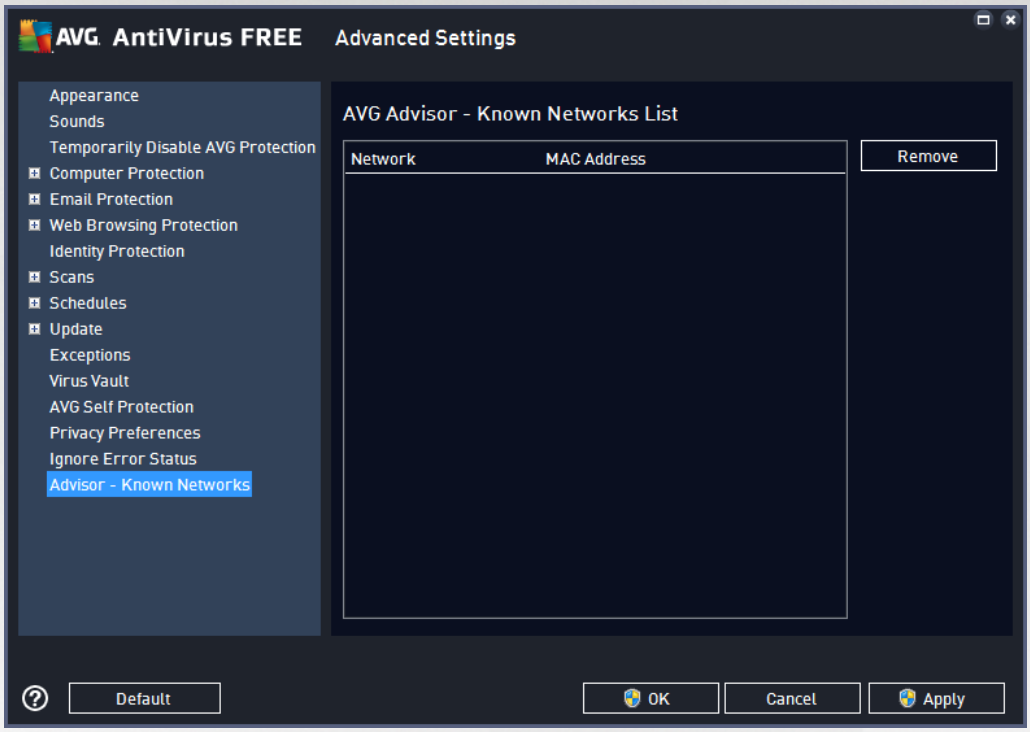
For this situation, within the ***Ignore error status*** dialog you can select components that may be in an error state (*or switched off*) and you do not wish to receive information about it. Press the ***OK*** button to confirm.

9.16. Advisor - Known Networks

The AVG Advisor includes a feature that monitors networks you connect to, and if a new network is found *(with an already used network name, which can lead to confusion)* it will notify you and recommend that you check the network's safety. If you decide that the new network is safe to connect to, you can also save it to this list *(Via the link provided in the AVG Advisor tray notification that slides over the system tray once an unknown network is detected. For details please see chapter on AVG Advisor)*. AVG Advisor will then remember the

unique attributes of the network *(specifically the MAC address)*, and will not display the notification next time. Each network that you connect to will be automatically considered the known network, and added to the list. You can delete individual entries by pressing the ***Remove*** button; the respective network will then be considered unknown and potentially unsafe again.

In this dialog window, you can check which networks are considered to be known:



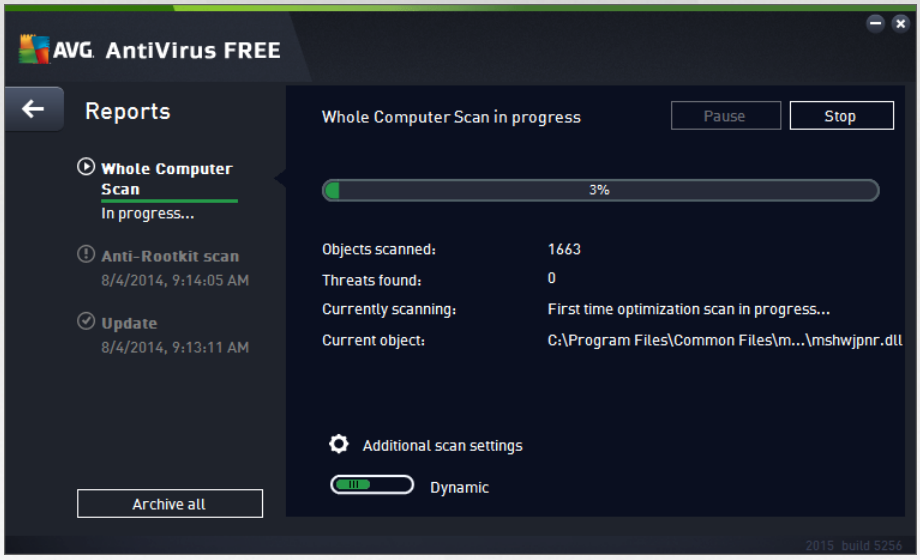
Note: *The known networks feature within AVG Advisor is not supported at Windows XP 64-bit.*

10. AVG Scanning

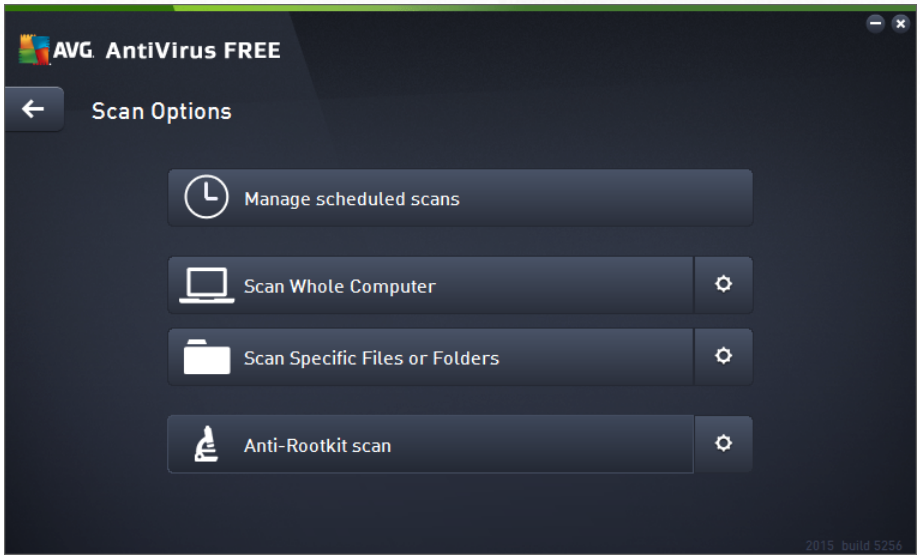
By default, **AVG AntiVirus Free Edition 2015** does not run any scans, as after the initial one *(that you will be invited to launch*), you should be perfectly protected by the resident components of **AVG AntiVirus Free Edition 2015** that are always on guard, and do no let any malicious code get into your computer. Of course, you can schedule a scan to run at regular intervals, or manually launch a scan according to your needs any time.

The AVG scanning interface is accessible from the main user interface via the button graphically divided into two sections:

- ***Scan now*** - Press the button to link to launch the Whole Computer Scan immediately, and watch its progress and results in the automatically opened Reports window:



- ***Options*** - Select this button *(graphically displayed as three horizontal lines in a green field)* to open the ***Scan Options*** dialog where you can manage scheduled scans and edit scan parameters:



In the ***Scan Options*** dialog, you can see three main scan configuration sections:

- ***Manage schedules scans*** - Click this option to open a new dialog with an overview of scan schedules. Unfortunately, within **AVG AntiVirus Free Edition 2015** you cannot define your own scans. Therefore you will only be able to see one scheduled scan predefined by the software vendor listed in the chart. The scan is turned off, by default. To turn it on, right-click on it and select the *Enable task* option from the context menu. Once the scheduled scan is enabled, you may edit its configuration via the *Edit scan schedule* button.

- ***Scan whole computer / Settings*** - The button is divided into two sections. Click the *Scan whole computer* option to immediately launch the scanning of the entire of your computer *(for details on the scan of the whole computer please see the respective chapter called Predefined scans / Scan whole computer)*. Clicking the bottom *Settings* section will take you to the configuration dialog of the whole computer scan.

- ***Scan specific files or folders / Settings*** - Again, the button is divided into two sections. Click the *Scan specific files or folders* option to immediately launch the scanning of selected areas of your computer *(for details on the scan of the selected files or folders please see the respective chapter called Predefined scans / Scan specific files or folders)*. Clicking the bottom *Settings* section will take you to the configuration dialog of the specific files or folders scan.

- ***Scan computer for rootkits / Settings*** - The left section of the button labeled *Scan computer for rootkits* launches the immediate anti-rootkit scanning *(for details on the rootkit scan please see the respective chapter called Predefined scans / Scan computer for rootkits)*. Clicking the *Settings* section will take you to the configuration dialog of the rootkit scan .

10.1. Predefined Scans

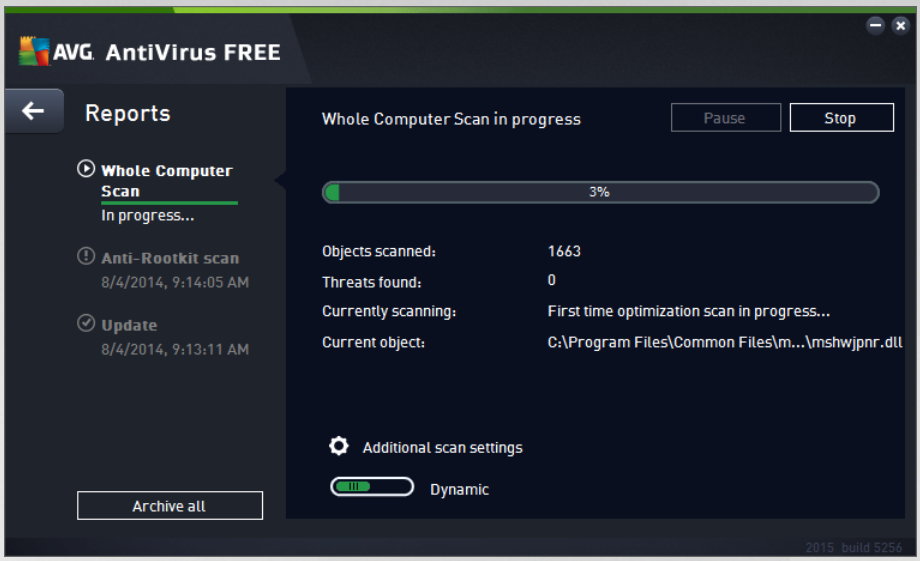
One of the main features of **AVG AntiVirus Free Edition 2015** is on-demand scanning. On-demand tests are designed to scan various parts of your computer whenever suspicion about possible virus infection arises. Anyway, it is strongly recommended that you carry out such tests regularly even if you think that no virus can be found on your computer. In the **AVG AntiVirus Free Edition 2015** you will find the following types of scan predefined by the software vendor:

10.1.1. Scan whole computer

Whole Computer scan scans your entire computer for possible infections and/or potentially unwanted applications. This test will scan all hard drives on your computer, will detect and heal any virus found, or remove the detected infection to the Virus Vault. Scanning the whole of your computer should be scheduled on your computer at least once a week.

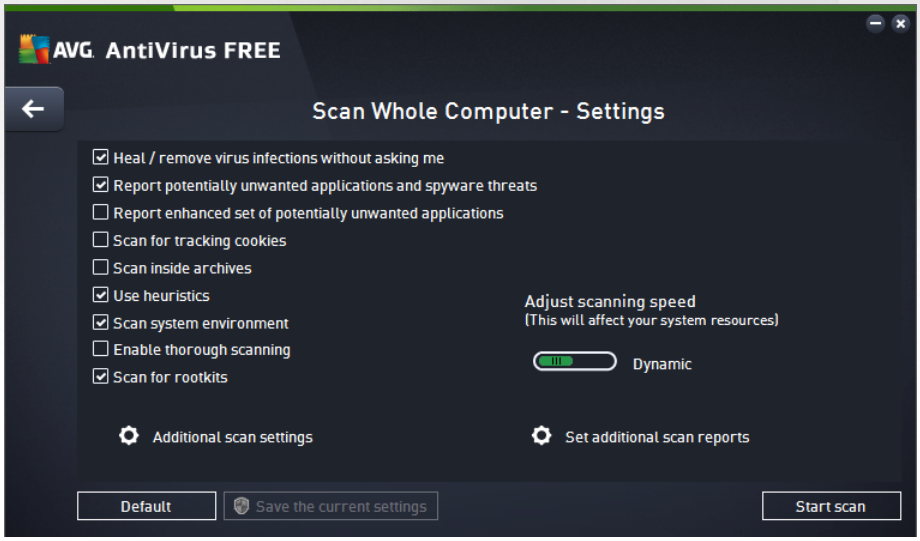
Scan launch

The ***Whole Computer scan*** can be launched directly from the main user interface by clicking on the ***Scan now*** button. No further specific settings have to be configured for this type of scan; the scan will start immediately. Within the ***Whole computer scan in progress*** dialog (*see screenshot*) you can watch its progress and results. The scan can be temporarily interrupted (***Pause***) or canceled (***Stop***) if needed.



Scan configuration editing

You can edit the ***Whole computer scan*** configuration in the ***Scan whole computer - Settings*** dialog *(the dialog is accessible via the Settings link for the Whole computer scan within the Scan options dialog).* ***It is recommended that you keep the default settings unless you have a valid reason to change them!***



In the list of scanning parameters you can switch on/off specific parameters as needed:

- ***Heal / remove virus infection without asking me*** *(on by default)* - If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default)* - Check to activate the scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer

security.

- ***Report enhanced set of potentially unwanted applications*** *(off by default)* - Mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan for tracking cookies*** *(off by default)* - This parameter specifies that cookies should be detected *(HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts)*.

- ***Scan inside archives*** *(off by default)* - This parameter specifies that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

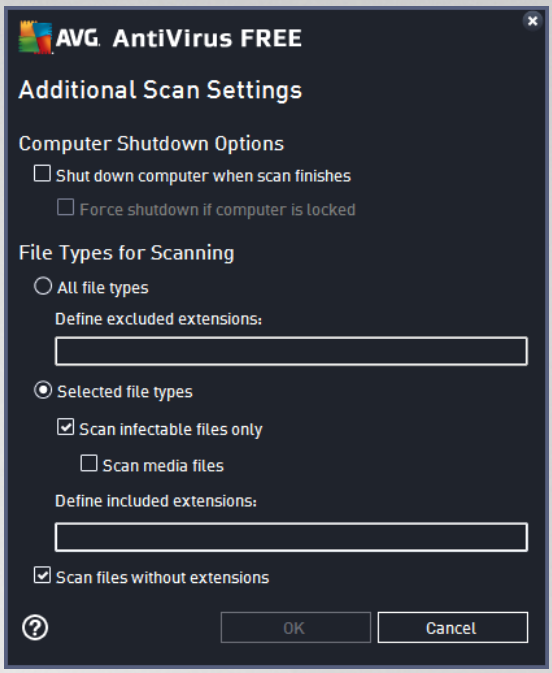
- ***Use Heuristics*** *(on by default)* - Heuristic analysis *(dynamic emulation of the scanned object's instructions in a virtual computer environment)* will be one of the methods used for virus detection during scanning.

- ***Scan system environment*** *(on by default)* - Scanning will also check the system areas of your computer.

- ***Enable thorough scanning*** *(off by default)* - In specific situations *(suspicions about your computer being infected)* you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.

- ***Scan for rootkits*** *(on by default)*: includes anti-rootkit scanning into the scanning of the whole computer. The anti-rootkit scan can be also launched separately.

- ***Additional scan settings*** - the link opens a new Additional scan settings dialog where you can specify the following parameters:



- ***Computer shutdown options*** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (***Shutdown computer upon scan completion***), a new option activates that allows the computer to shut down even if it is currently locked (***Force shutdown if computer is locked***).

- ***File types for scanning*** - you should also decide whether you want scan:

  - ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned;

  - ***Selected file types*** - you can specify that you want to scan only files that can be infected (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not likely to be infected by a virus*). Again, you can specify by extensions which files should always be scanned.

  - Optionally, you can decide to ***Scan files without extension*** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

- ***Adjust how quickly scan completes*** - you can use the slider to change the scanning process priority. By default, this option value is set to the *user sensitive* level of automatic resource usage. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resource requirements (*e.g. when the computer is temporarily unattended*).

- ***Set additional scan reports*** - the link opens a new ***Scan reports*** dialog where you can select what types of possible findings should be reported:

Warning: *These scan settings are identical to the parameters for a newly defined scan - as described in the AVG Scanning / Scan scheduling/ How to Scan chapter. Should you decide to change the default configuration of the* ***Scan the whole computer*** *you can then save your new setting as the default configuration to be used for all further scans for the whole computer.*

10.1.2. Scan specific files or folders

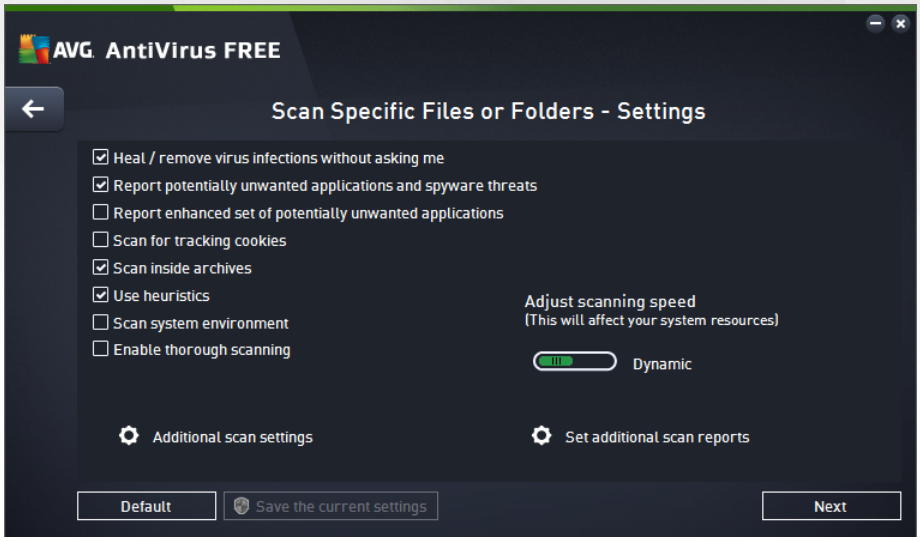
Scan specific files or folders - scans only those areas of your computer that you have selected to be scanned (*selected folders, hard disks, floppy discs, CDs, etc.*). The scanning progress in case of virus detection and its treatment is the same as when scanning the whole computer: any virus found is healed or removed to the Virus Vault. Specific files or folders scanning can be used to set up your own tests and their scheduling based on your needs.

Scan launch

The ***Scan of specific files or folders*** can be launched directly from the Scan options dialog by clicking on the **Scan specific files or folders** button. A new dialog called ***Select specific files or folders for scanning*** opens. In the tree structure of your computer select those folders you want to scan. The path to each selected folder will be generated automatically and appear in the text box in the upper part of this dialog. There is also the option of having a specific folder scanned while all its sub folders are excluded from this scan; to do that write a minus sign "**-**" in front of the automatically generated path (*see screenshot*). To exclude the entire folder from scanning use the "!" parameter. Finally, to launch the scan, press the ***Start scan*** button; the scanning process itself is basically identical to the Whole computer scan.

Scan configuration editing

You can edit the ***Scan specific files or folders*** configuration in the ***Scan specific files or folders - Settings*** dialog *(the dialog is accessible via the Settings link for the Scan specific files or folders within the Scan options dialog).* ***It is recommended that you keep the default settings unless you have a valid reason to change them!***



In the list of scanning parameters you can switch specific parameters on/off as needed:

- ***Heal / remove virus infection without asking me*** *(on by default)*: If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.

- ***Report potentially unwanted applications and spyware threats*** *(on by default)*: Check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed

intentionally. We recommend that you keep this feature activated as it increases your computer security.

- ***Report enhanced set of potentially unwanted applications*** *(off by default)*: Mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.

- ***Scan for Tracking Cookies*** *(off by default)*: This parameter specifies that cookies should be detected *(HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts)*.

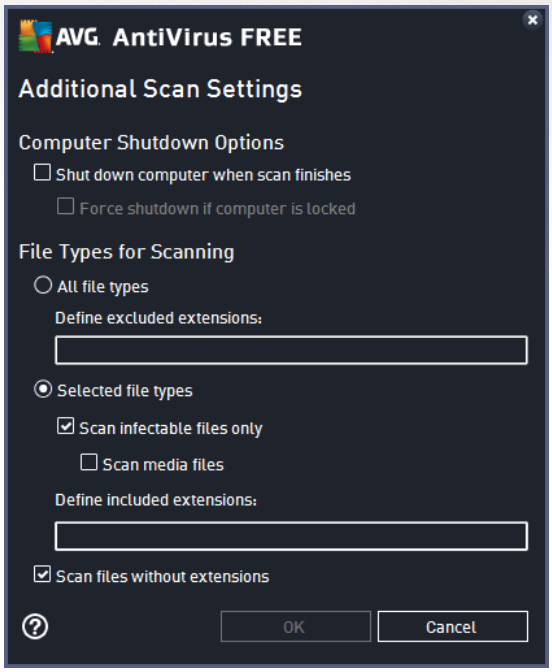
- ***Scan inside archives*** *(on by default)*: This parameters defines that scanning should check all files stored inside archives, e.g. ZIP, RAR, ...

- ***Use Heuristics*** *(on by default)*: Heuristic analysis *(dynamic emulation of the scanned object's instructions in a virtual computer environment)* will be one of the methods used for virus detection during scanning.

- ***Scan system environment*** *(off by default)*: Scanning will also check the system areas of your computer.

- ***Enable thorough scanning*** *(off by default)*: In specific situations *(suspicions about your computer being infected)* you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.

- ***Additional scan settings*** - The link opens a new ***Additional scan settings*** dialog where you can specify the following parameters:



- **Computer shutdown options** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option (**Shutdown computer upon scan completion**), a new option activates that allows the computer to shut down even if it is currently locked (**Force shutdown if computer is locked**).

- **File types for scanning** - you should also decide whether you want to scan:

  - **All file types** with the option of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned;

  - **Selected file types** - you can specify that you want to scan only files that can be infected (*files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files*), including media files (*video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not likely to be infected by a virus*). Again, you can specify by extensions which files should always be scanned.

  - Optionally, you can decide to **Scan files without extension** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

- **Adjust how quickly scan completes** - you can use the slider to change the scanning process priority. By default, this option value is set to the *user sensitive* level of automatic resource usage. Alternatively, you can run the scanning process slower which means the system resources load will be minimized (*useful when you need to work on the computer but you do not care so much how long the scanning takes*), or faster with increased system resources requirements (*e.g. when the computer is temporarily unattended*).

- **Set additional scan reports** - the link opens a new **Scan Reports** dialog where you can select what types of potential findings should be reported:

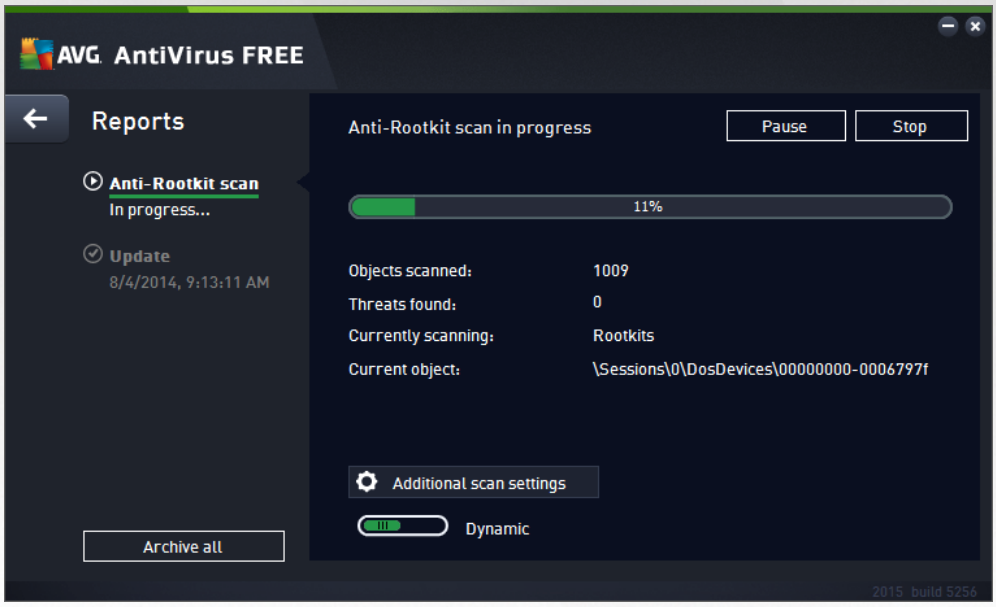
Warning: *These scan settings are identical to the parameters for a newly defined scan - as described in the AVG Scanning / Scan scheduling/ How to Scan chapter. Should you decide to change the default configuration of the* **Scan specific files or folders** *you can then save your new setting as the default configuration to be used for all further scans of specific files or folders. Also, this configuration will be used as a template for all of your newly scheduled scans (all customized scans are based on the current configuration of the Scan of selected files or folders).*

10.1.3. Scan computer for rootkits

Scan computer for rootkits is detecting and effectively removing dangerous rootkits, i.e. programs and technologies that can camouflage the presence of malicious software on your computer. A rootkit is designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. The scan is able to detect rootkits based on a predefined set of rules. If a rootkit is found, it does not necessarily mean it is infected. Sometimes, rootkits are used as drivers or they are a part of correct applications.

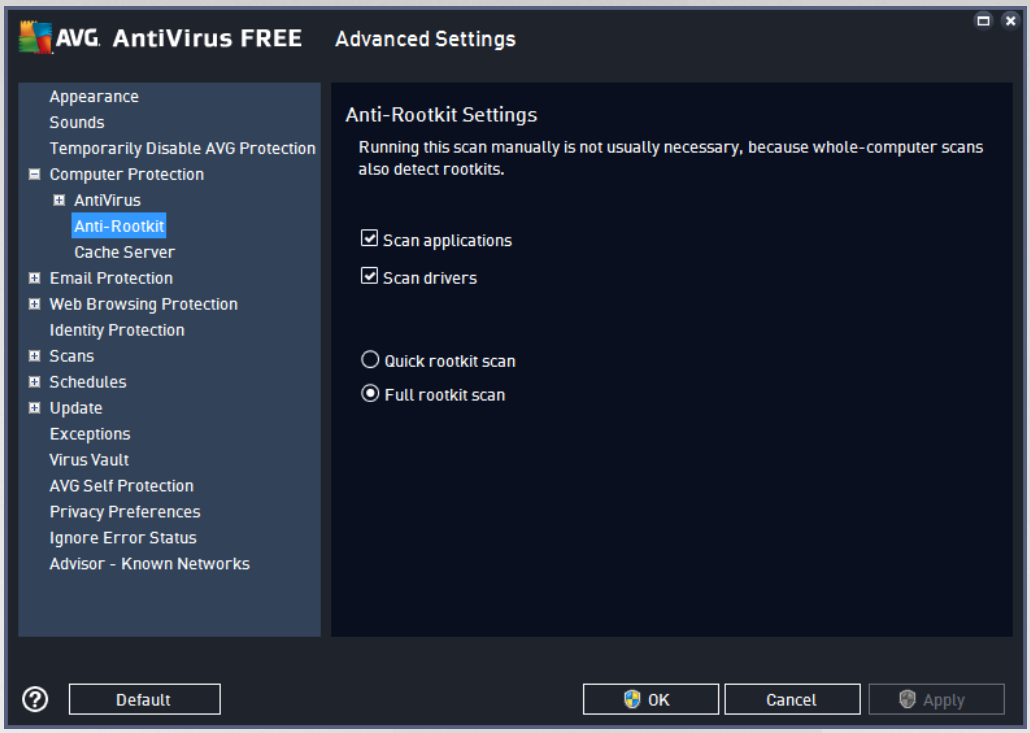
Scan launch

Scan computer for rootkits can be launched directly from the Scan options dialog by clicking on the ***Scan computer for rootkits*** button. A new dialog called ***Anti-rootkit scan in progress*** opens showing the progress of the launched scan:



Scan configuration editing

You can edit the Anti-Rootkit scan configuration in the ***Anti-Rootkit Settings*** dialog *(the dialog is accessible via the Settings link for the Scan computer for rootkits scan within the Scan options dialog).* ***It is recommended that you keep the default settings unless you have a valid reason to change them!***

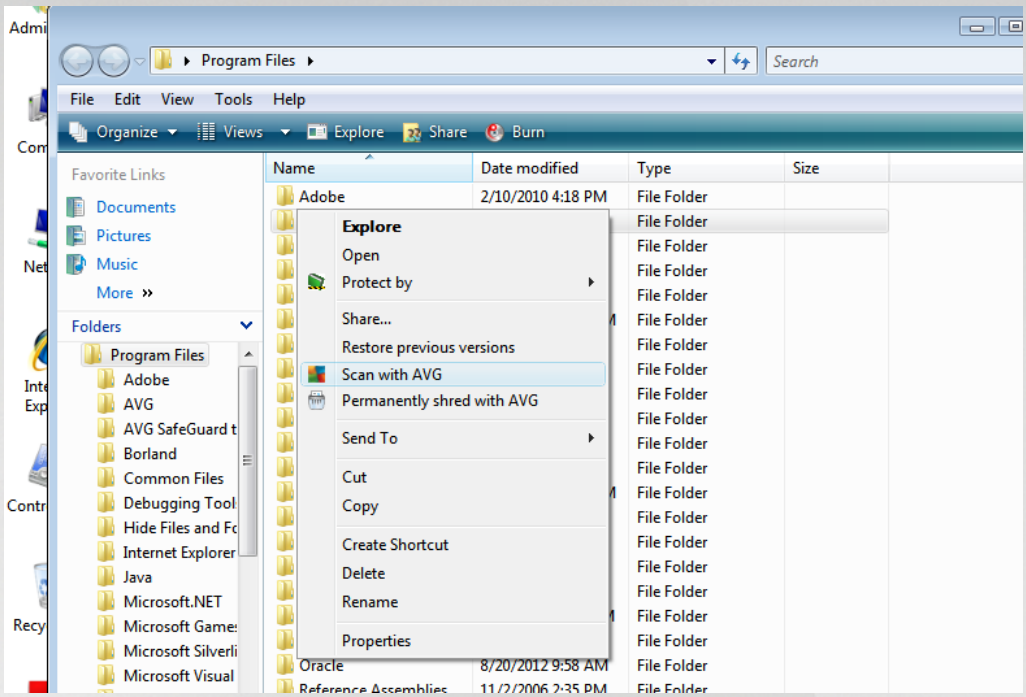


Scan applications and ***Scan drivers*** enable you to specify in detail what should be included in anti-rootkit scanning. These settings are intended for advanced users; we recommend that you keep all options switched on. You can also pick the rootkit scanning mode:

- ***Quick rootkit scan*** - scans all running processes, loaded drivers and the system folder (*typically c:\Windows*)
- ***Full rootkit scan*** - scans all running processes, loaded drivers, the system folder (*typically c:\Windows*), plus all local disks (*including the flash disk, but excluding floppy disk/CD drives*)

10.2. Scanning in Windows Explorer

Besides the pre-defined scans launched for the entire computer or its selected areas, **AVG AntiVirus Free Edition 2015** also offers the option of quick scanning of a specific object directly in the Windows Explorer environment. If you want to open an unknown file and you cannot be sure of its content, you may want to have it checked on demand. Follow these steps:



- Within Windows Explorer highlight the file *(or folder)* you want to check
- Right-click your mouse over the object to open the context menu
- Select the ***Scan with AVG*** option to have the file scanned with **AVG AntiVirus Free Edition 2015**

10.3. Command Line Scanning

Within **AVG AntiVirus Free Edition 2015** there is the option of running the scan from the command line. You can use this option for instance on servers, or when creating a batch script to be launched automatically after the computer boot. From the command line, you can launch the scan with most parameters as offered in the AVG graphical user interface.

To launch the AVG scan from the command line, run the following command within the folder where AVG is installed:

- ***avgscanx*** for 32 bits OS
- ***avgscana*** for 64 bits OS

Syntax of the command

The syntax of the command follows:

- ***avgscanx /parameter*** ... e.g. ***avgscanx /comp*** for scanning the whole computer
- ***avgscanx /parameter /parameter*** .. with multiple parameters these should be lined up in a row and separated by a space and a slash character

- if a parameter requires specific value to be provided (e.g. the ***/scan*** parameter that requires information on the selected areas of your computer that are to be scanned, and you have to provide an exact path to the selected section), the values are separated by semicolons, for instance: ***avgscanx /scan=C:\;D:***

Scanning parameters

To display a complete overview of available parameters, type the respective command together with the parameter /? or /HELP (e.g. ***avgscanx /?***). The only obligatory parameter is /SCAN to specify what areas of the computer should be scanned. For a more detailed explanation of the options, see the command line parameters overview.

To run the scan press ***Enter***. During scanning you can stop the process using ***Ctrl+C*** or ***Ctrl+Pause***.

CMD scanning launched from graphic interface

When you run your computer in Windows Safe Mode, there is also an option to launch the command line scan from the graphic user interface. The scan itself will be launched from the command line, the ***Command Line Composer*** dialog only allows you to specify most scanning parameters in the comfortable graphic interface.

Since this dialog is only accessible within the Windows Safe Mode, for a detailed description of this dialog please consult the help file opened directly from the dialog.

10.3.1. CMD Scan Parameters

There follows a list of all parameters available for command line scanning:

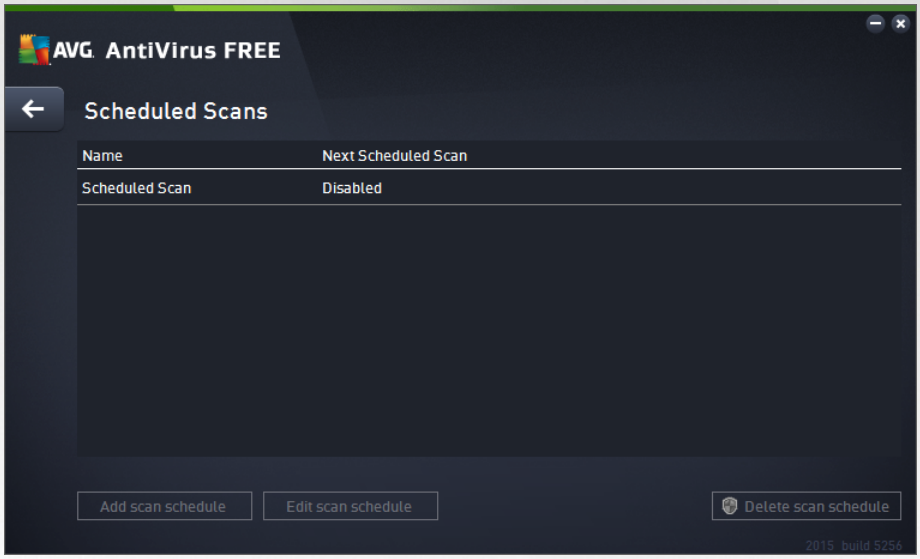
- /SCAN Scan specific files or folders /SCAN=path;path *(e.g. /SCAN=C:\;D:\)*
- /COMP Whole Computer scan
- /HEUR Use heuristic analysis
- /EXCLUDE Exclude path or files from scan
- /@ Command file /file name/
- /EXT Scan these extensions /for example EXT=EXE,DLL/
- /NOEXT Do not scan these extensions /for example NOEXT=JPG/
- /ARC Scan archives
- /CLEAN Clean automatically
- /TRASH Move infected files to the Virus Vault
- /QT Quick test
- /LOG Generate a scan result file

- /MACROW Report macros
- /PWDW Report password-protected files
- /ARCBOMBSW Report archive bombs *(repeatedly compressed archives)*
- /IGNLOCKED Ignore locked files
- /REPORT Report to file /file name/
- /REPAPPEND Append to the report file
- /REPOK Report uninfected files as OK
- /NOBREAK Do not allow CTRL-BREAK to abort
- /BOOT Enable MBR/BOOT check
- /PROC Scan active processes
- /PUP Report Potentially unwanted programs
- /PUPEXT Report enhanced set of Potentially unwanted programs
- /REG Scan registry
- /COO Scan cookies
- /? Display help on this topic
- /HELP Display help on this topic
- /PRIORITY Set scan priority /Low, Auto, High/ *(see Advanced settings / Scans)*
- /SHUTDOWN Shutdown computer upon scan completion
- /FORCESHUTDOWN Force computer shutdown upon scan completion
- /ADS Scan Alternate Data Streams *(NTFS only)*
- /HIDDEN Report files with hidden extensions
- /INFECTABLEONLY Scan files with infectable extensions only
- /THOROUGHSCAN Enable thorough scanning
- /CLOUDCHECK Check for false positives
- /ARCBOMBSW Report re-compressed archive files

10.4. Scan Scheduling

With **AVG AntiVirus Free Edition 2015** you can run scan on demand *(for instance when you suspect an infection has penetrated your computer)* or based on a scheduled plan. It is highly recommended that you run the scans based on a schedule: this way you can make sure your computer is protected from any possibility of getting infected, and you will not have to worry about if and when to launch the scan. You should launch the Whole Computer scan regularly, at least once a week. However, if possible, launch the scan of your entire computer daily - as set up in the scan schedule default configuration. If the computer is "always on" then you can schedule scans out of working hours. If the computer is sometimes switched off, then schedule scans to occur on computer start-up when the task has been missed.

The scan schedule can be created / edited in the ***Scheduled scans*** dialog that is accessible via the ***Manage scheduled scan*** button within the Scan options dialog. In the new ***Scheduled Scan*** dialog you can see a complete overview of all currently scheduled scans:

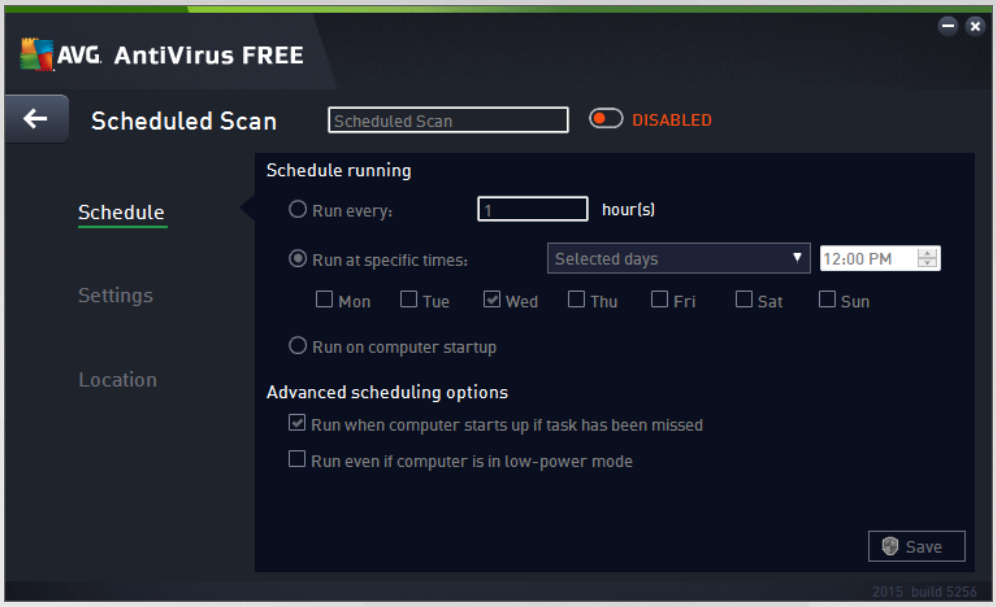


Before you define your own scans, you will only be able to see one scheduled scan predefined by the software vendor listed in the chart. The scan is turned off, by default. To turn it on, right-click on it and select the ***Enable task*** option from the context menu. Once the scheduled scan is enabled, you may edit its configuration via the ***Edit scan schedule*** button. You can also click the ***Add scan schedule*** button to create a new scan schedule of your own. The parameters of the scheduled scan can be edited (*or a new schedule set up*) on three tabs:

- Schedule
- Settings
- Location

On each tab you can simply switch the "traffic light" button to deactivate the scheduled test temporarily, and switch it on again as the need arises:

10.4.1. Schedule



In the upper part of the ***Schedule*** tab you can find the text field where you can specify the name of the scan schedule that is currently being defined. Try to always use brief, descriptive, and apt names for scans to make it easier to later differentiate the scan from others. For example, it is not appropriate to call the scan by the name "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System area scan" etc.

In this dialog you can further define the following parameters of the scan:

- ***Schedule running*** - Here, you can specify time intervals for the newly scheduled scan launch. The timing can either be defined by the repeated scan launch after a certain period of time *(Run every ...)* or by defining an exact date and time *(Run at specific times)*, or possibly by defining an event that the scan launch should be associated with *(Run on computer startup)*.

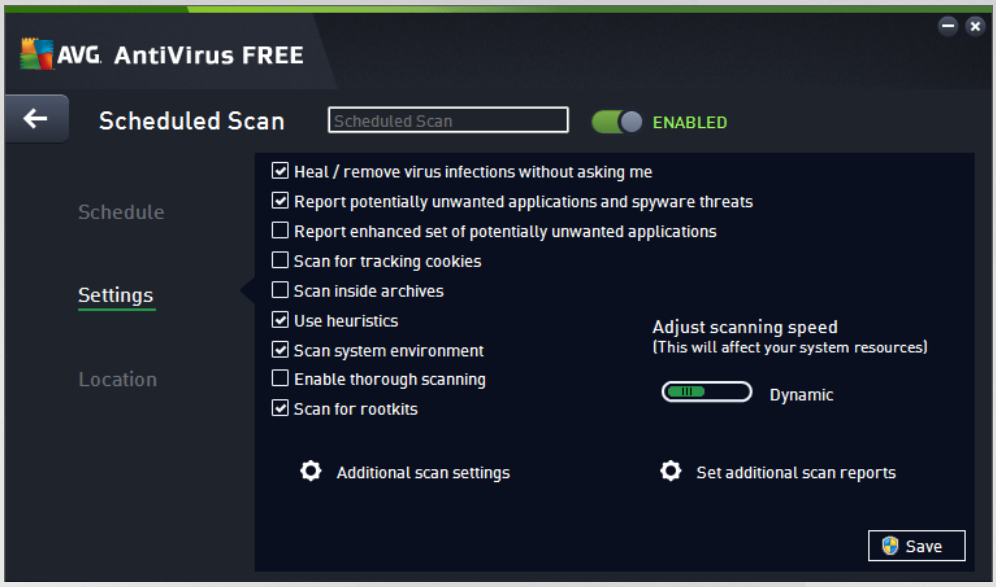
- ***Advanced schedule options*** - This section allows you to define under which conditions the scan should/should not be launched if the computer is in low power mode or switched off completely. Once the scheduled scan is launched in the time you have specified, you will be informed on this fact via a pop-up window opened over the AVG system tray icon. A new AVG system tray icon then appears (in full color with a flash light) informing a scheduled scan is running. Right-click on the running scan AVG icon to open a context menu where you can decide to pause or even stop the running scan, and also change the priority of the currently running scan.

Controls in the dialog

- ***Save*** - Saves all changes you have performed on this tab or on any other tab on this dialog, and switches back to the Scheduled scans overview. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.

- - Use the green arrow in the upper left section of the dialog to get back to the Scheduled scans overview.

10.4.2. Settings



In the upper part of the ***Settings*** tab you can find the text field where you can specify the name of the scan schedule that is currently being defined. Try to always use brief, descriptive, and apt names for scans to make it easier to later differentiate the scan from others. For example, it is not appropriate to call the scan by the name "New scan" or "My scan" since these names do not refer to what the scan actually checks. On the other hand, an example of a good descriptive name would be "System area scan" etc.

On the ***Settings*** tab you will find a list of scanning parameters that can be optionally switched on/off. ***Unless you have a valid reason to change these settings we recommend that you keep the predefined configuration***:

- ***Heal / remove virus infection without asking me*** *(on by default):* if a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be moved to the Virus Vault.
- ***Report potentially unwanted applications and spyware threats*** *(on by default):* check to activate scanning for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend that you keep this feature activated as it increases your computer security.
- ***Report enhanced set of potentially unwanted applications*** (*off by default*): mark to detect extended packages of spyware: programs that are perfectly ok and harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases your computer security even more, however it may block legal programs, and is therefore switched off by default.
- ***Scan for Tracking Cookies*** (*off by default*): this parameter specifies that cookies should be detected during scanning; (*HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts*)
- ***Scan inside archives*** (*off by default*): this parameter specifies that the scanning should check all files even if they are stored inside an archive, e.g. ZIP, RAR, ...

- ***Use Heuristics*** (*on by default*): heuristic analysis (*dynamic emulation of the scanned object's instructions in a virtual computer environment*) will be one of the methods used for virus detection during scanning;

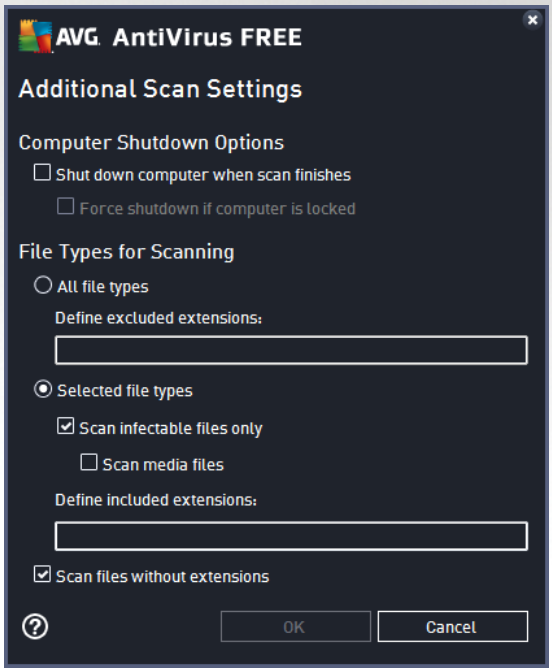
- ***Scan system environment*** (*on by default*): scanning will also check the system areas of your computer;

- ***Enable thorough scanning*** (*off by default):* in specific situations (*suspicious of your computer being infected*) you may check this option to activate the most thorough scanning algorithms that will scan even those areas of your computer that rarely get infected, just to be absolutely sure. Remember though that this method is rather time-consuming.

- ***Scan for rootkits*** *(on by default):* Anti-Rootkit scan searches your computer for possible rootkits, i.e. programs and technologies that can cover malware activity in your computer. If a rootkit is detected, this does not necessarily mean your computer is infected. In some cases, specific drivers or sections of regular applications may be misleadingly detected as rootkits.

Additional scan settings

The link opens a new ***Additional Scan Settings*** dialog where you can specify the following parameters:



- ***Computer shutdown options*** - decide whether the computer should be shut down automatically once the running scanning process is over. Having confirmed this option *(Shutdown computer upon scan completion)*, a new option activates that allows the computer to shut down even if it is currently locked *(Force shutdown if computer is locked)*.

- ***File types for scanning*** - you should also decide whether you want to scan:

    - ***All file types*** with the option of defining exceptions from scanning by providing a list of comma separated file extensions that should not be scanned;

- **Selected file types** - you can specify that you want to scan only files that can be infected *(files that cannot get infected will not be scanned, for instance some plain text files, or some other non-executable files)*, including media files *(video, audio files - if you leave this box unchecked, it will reduce the scanning time even more, because these files are often quite large and are not too likely to be infected by a virus)*. Again, you can specify by extensions which files should always be scanned.

- Optionally, you can decide you want to **Scan files without extension** - this option is on by default, and it is recommended that you keep it so unless you have a real reason to change it. Files with no extensions are rather suspicious and should be scanned at all times.

Adjust how quickly scan completes

Within this section you can further specify the desired scanning speed dependent on system resource usage. By default, this option value is set to the *user sensitive* level of automatic resource usage. If you want the scan to run faster, it will take less time but the system resources used will increase significantly during the scan, and will slow down your other activities on the PC (*this option can be used when your computer is switched on but nobody is currently working on it*). On the other hand, you can decrease the system resources used by extending the scanning duration.

Set additional scan reports

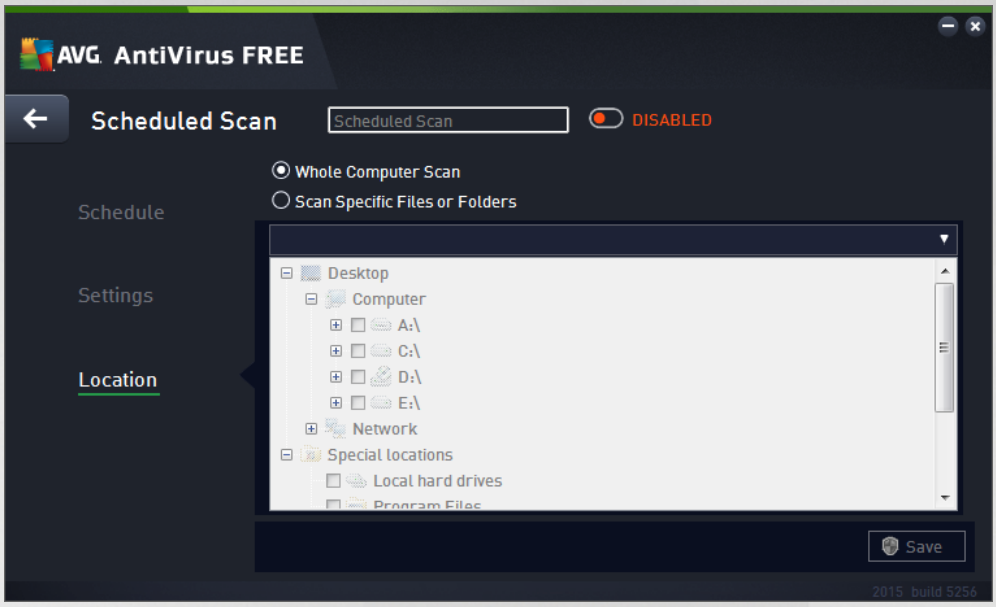
Click the **Set additional scan reports ...** link to open a standalone dialog window called **Scan reports** where you can tick several items to define what scan findings should be reported:

Controls in the dialog

- **Save** - Saves all changes you have performed on this tab or on any other tab on this dialog, and switches back to the Scheduled scans overview. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.

- - Use the green arrow in the upper left section of the dialog to get back to the Scheduled scans overview.

10.4.3. Location



On the ***Location*** tab you can define whether you want to schedule scanning of the whole computer or scanning of specific files or folders. In case you select scanning of specific files or folders, in the bottom part of this dialog the displayed tree structure activates and you can specify the folders to be scanned (*expand items by clicking the plus node until you find the folder you wish to scan*). You can select multiple folders by checking the respective boxes. The selected folders will appear in the text field on the top of the dialog, and the drop-down menu will keep your selected scan history for later use. Alternatively, you can enter the full path to the desired folder manually (*if you enter multiple paths, it is necessary to separate with semi-colons without extra spaces*).

Within the tree structure you can also see a branch called ***Special locations***. Below is a list of locations that will be scanned once the respective checkbox is marked:

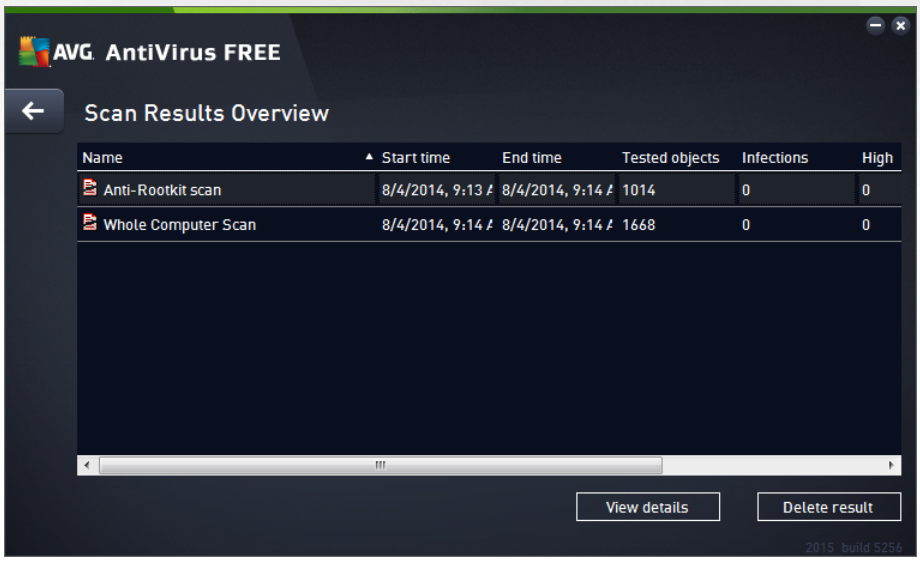
- ***Local hard drives*** - all hard drives of your computer
- ***Program files***
    - C:\Program Files\
    - *in 64-bit version* C:\Program Files (x86)
- ***My Documents folder***
    - *for Win XP:* C:\Documents and Settings\Default User\My Documents\
    - *for Windows Vista/7*: C:\Users\user\Documents\
- ***Shared Documents***
    - *for Win XP*: C:\Documents and Settings\All Users\Documents\
    - *for Windows Vista/7*: C:\Users\Public\Documents\

- ***Windows folder*** - C:\Windows\
- ***Other***
    - *System drive* - the hard drive on which the operating system is installed (usually C:)
    - *System folder* - C:\Windows\System32\
    - *Temporary Files folder* - C:\Documents and Settings\User\Local\ (*Windows XP*); or C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
    - *Temporary Internet Files* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); or C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Controls in the dialog

- ***Save*** - Saves all changes you have performed on this tab or on any other tab on this dialog, and switches back to the Scheduled scans overview. Therefore if you wish to configure the test parameters on all tabs, press the button to save them only after you have specified all your requirements.
- - Use the green arrow in the upper left section of the dialog to get back to the Scheduled scans overview.

10.5. Scan Results



The ***Scan results overview*** dialog provides a list of results of all so far performed scans. The chart provides the following information on each scan result:

- ***Icon*** - The first column displays an information icon describing the status of the scan:
    - No infections found, scan completed

- No infections found, scan was interrupted before completion
- Infections were found and not healed, scan completed
- Infections were found and not healed, scan was interrupted before completion
- Infections found and all were healed or removed, scan completed
- Infections found and all were healed or removed, scan was interrupted before completion

- ***Name*** - The column provides the name of the respective scan. Either it is one of the two predefined scans, or your own scheduled scan.
- ***Start time*** - Gives the exact date and time the scan was launched.
- ***End time*** - Gives the exact date and time the scan finished, was paused, or interrupted.
- ***Tested objects*** - Provides the total number of all objects that were scanned.
- ***Infections*** - Gives the number of removed/total infections found.
- ***High / Medium / Low*** - The subsequent three columns give the number of high, medium and low severity infections found respectively.
- ***Rootkits*** - Provides the total number of rootkits found during the scanning.

Dialog controls

View details - Click the button to see detailed information about a selected scan *(highlighted in the chart above)*.

Delete results - Click the button to remove a selected scan result information from the chart.

- Use the green arrow in the upper left section of the dialog to get back to the main user interface with the components' overview.

10.6. Scan results details

To open an overview of detailed information on a selected scan result, click the ***View details*** button accessible in the Scan results overview dialog. You will get redirected to the same dialog interface describing in details the information on a respective scan result. The information is divided on three tabs:

- ***Summary*** - The tab gives basic information about the scan: If it was completed successfully, if any threats were found and what happened to them.
- ***Details*** - The tab displays all information about the scan, including details about any detected threats. Export overview to file enables you to save it as a .csv file.
- ***Detections*** - This tab is only displayed if there were any threats detected during the scan, and gives detailed information about the threats:

Low severity: information or warnings, not real threats. Typically documents containing macros, documents or archives protected by a password, locked files, etc.

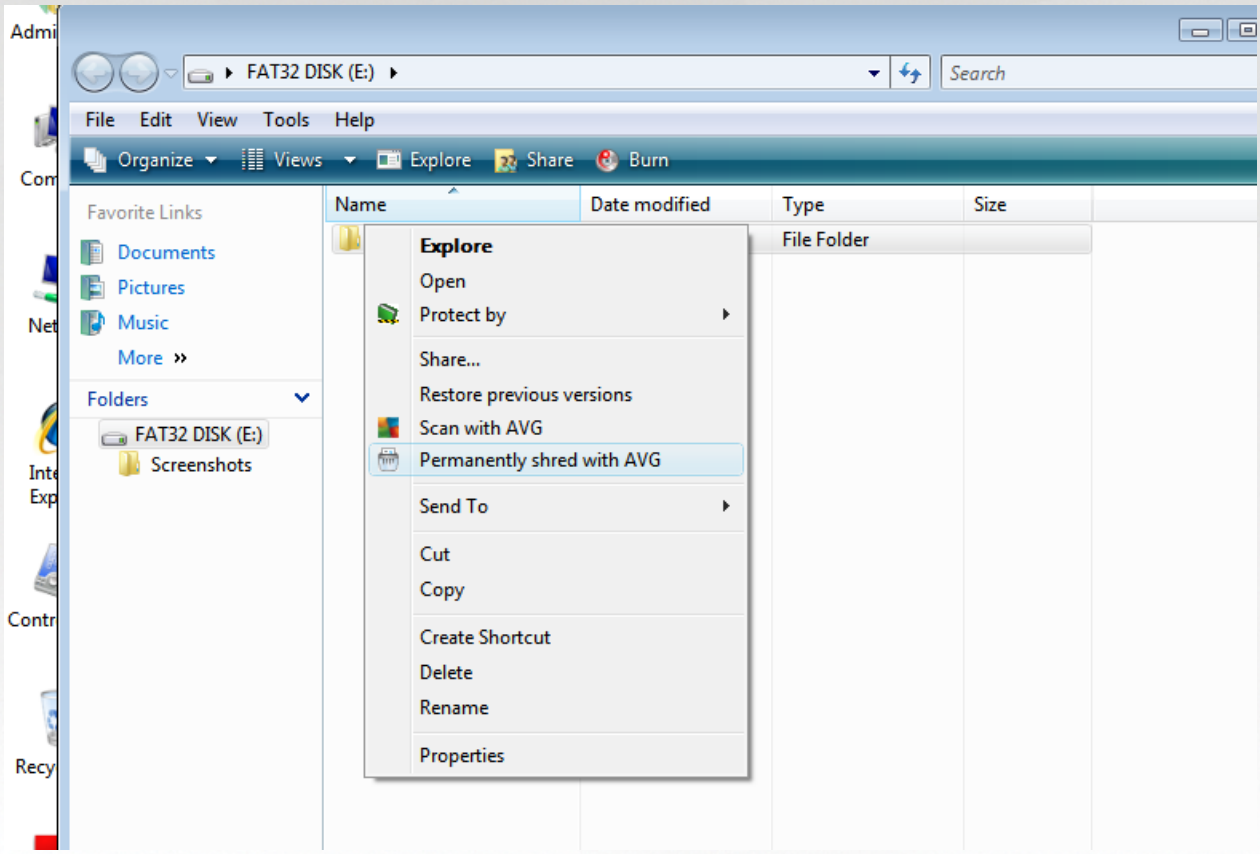
Medium severity: typically potentially unwanted applications, such as adware or tracking cookies

High severity: serious threats such as viruses, Trojans, exploits, etc. Also objects detected by the Heuristics detection method, i.e. threats not yet described in the virus database.

11. AVG File Shredder

AVG File Shredder has been designed to delete files absolutely securely, that is with no chance to recover them, even with advanced software tools for this purpose.

To shred a file or folder, right-click it in a file manager *(Windows Explorer, Total Commander, ...)* and select ***Permanently shred with AVG*** in the context menu. Files in the Recycle Bin can be shredded as well. If a specific file in a specific location *(e.g. CD-ROM)* cannot be shredded reliably, you will be notified, or the option in the context menu will not be available at all.



Please always bear in mind: Once you shred a file, it is gone forever.

12. Virus Vault

Virus Vault is a safe environment for the management of suspect/infected objects detected during AVG tests. Once an infected object is detected during scanning, and AVG is not able to heal it automatically, you are asked to decide what is to be done with the suspect object. The recommended solution is to move the object to the ***Virus Vault*** for further treatment. The main purpose of the ***Virus Vault*** is to keep any deleted file for a certain period of time, so that you can make sure you do not need the file any more in its original location. Should you find out the file absence causes problems, you can send the file in question to analysis, or restore it to the original location.

The ***Virus vault*** interface opens in a separate window and offers an overview of the information on quarantined infected objects:

- ***Date Added*** - Provides date and time the suspected file was detected and removed to the Virus Vault.
- ***Threat*** - In case you decided to install the Identity component within your **AVG AntiVirus Free Edition 2015**, a graphical identification of the finding severity will be provided in this section: from unobjectionable *(three green dots)* up to very dangerous *(three red dots).* Also you will find information on the infection type and its original location. The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia.
- ***Source*** - Specifies which component of **AVG AntiVirus Free Edition 2015** has detected the respective threat.
- ***Notifications*** - In a very rare situation, some notes may occur in this column providing detailed comments on the respective detected threat.

Control buttons

The following control buttons are accessible from the ***Virus Vault*** interface:

- ***Restore*** - removes the infected file back to its original location on your disk.
- ***Restore As*** - moves the infected file to a selected folder.
- ***Send to analysis*** - the button is only active when you highlight an object in the list of detections above. In such case, you have the option to send the selected detection to the AVG virus labs for further detailed analysis. Please note that this feature should primarily serve for sending false positives, i.e. files that have been detected by AVG as infected or suspicious, but which you believe are harmless.
- ***Details*** - for detailed information on the specific threat quarantined in the ***Virus Vault*** highlight the selected item in the list and click the ***Details*** button to call a new dialog with a description of the detected threat.
- ***Delete*** - removes the infected file from the ***Virus Vault*** completely and irreversibly.
- ***Empty Vault*** - removes all ***Virus Vault*** content completely. By removing the files from the ***Virus Vault***, these files are irreversibly removed from the disk (*not moved to the recycle bin*).

13. History

The ***History*** section includes information on all past events *(such as updates, scans, detections, etc.)* and reports about these events. This section is accessible from the main user interface via the ***Options / History*** item. Further, the history of all recorded events is divided into the following parts:

- Scan Results
- Resident Shield Results
- Email Protection Results
- Event History

13.1. Scan results

The ***Scan results overview*** dialog is accessible via the ***Options / History / Scan results*** menu item in the upper line navigation of the **AVG AntiVirus Free Edition 2015** main window. The dialog provides a list of all previously launched scans and information on their results:

- ***Name*** - scan designation; it can either be the name of one of the predefined scans, or a name you have given to your own scheduled scan. Every name includes an icon indicating the scan result:

  - green icon informs there was no infection detected during the scan

  - blue icon announces there was an infection detected during the scan but the infected object was removed automatically

  - red icon warns there was an infection detected during the scan and it could not be removed!

  Each icon can either be solid or cut in half - the solid icons stands for a scan that was completed and finished properly; the cut-in-half icon means the scan was canceled or

interrupted.

Note: *For detailed information on each scan please see the Scan Results dialog accessible via the View details button (in the bottom part of this dialog).*

- ***Start time*** - date and time when the scan was launched
- ***End time*** - date and time when the scan ended
- ***Tested objects*** - number of objects that were checked during scanning
- ***Infections*** - number of virus infections detected / removed
- ***High / Medium*** - these columns give the number of removed/total infections found of high, and medium severity respectively
- ***Info*** - information relating to the scanning course and result *(typically on its finalization or interruption)*
- ***Rootkits*** - number of detected rootkits

Control buttons

The control buttons for the ***Scan results overview*** dialog are:

- ***View details*** - press it to switch to the Scan results dialog to view detailed data on the selected scan
- ***Delete result*** - press it to remove the selected item from the scan results overview
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog

13.2. Resident Shield Results

The ***Resident Shield*** service is a part of the ***Computer*** component and scans files as they are copied, opened, or saved. When a virus or any kind of threat is detected, you will be warned immediately via the following dialog:

AVG AntiVirus FREE
AVG Detection
Threat: Virus identified EICAR_Test [More info]
Object name: c:\Users\Administrator\Documents\EICAR.COM
Protect Me (recommended)
AVG will choose the best method for removing this threat.
Ignore threat
AVG will prevent you from accessing the infected file. The threat will not be removed.
Show details

Within this warning dialog you will find information on the object that was detected and assigned as infected (*Threat*), and some descriptive facts on the recognized infection (*Object name*). The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia, if these are known. In the dialog, you will also see an overview of available solutions on how to treat the detected threat. One of the alternatives will be labeled as recommended: ***Protect Me (recommended). If possible, you should always stick to this option!***

Note: *It may happen that the size of the detected object exceeds the free space limit in the Virus Vault. If so, a warning message pops up informing you about the issue as you try to move the infected object to the Virus Vault. However, the Virus Vault size can be modified. It is defined as an adjustable percentage of the real size of your hard disk. To increase the size of your Virus Vault, go to the Virus Vault dialog within the AVG Advanced Settings, via the 'Limit Virus Vault size' option.*

In the bottom section of the dialog you can find the ***Show details*** link. Click it to open a new window with detailed information on the process running while the infection was detected, and the process' identification.

A list of all Resident Shield detections is available for overview within the ***Resident Shield detection*** dialog. This dialog is accessible via the ***Options / History / Resident Shield detection*** menu item in the upper line navigation of the **AVG AntiVirus Free Edition 2015** main window. The dialog offers an overview of objects that were detected by the resident shield evaluated as dangerous and either cured or moved to the Virus Vault.

For each detected object the following information is provided:

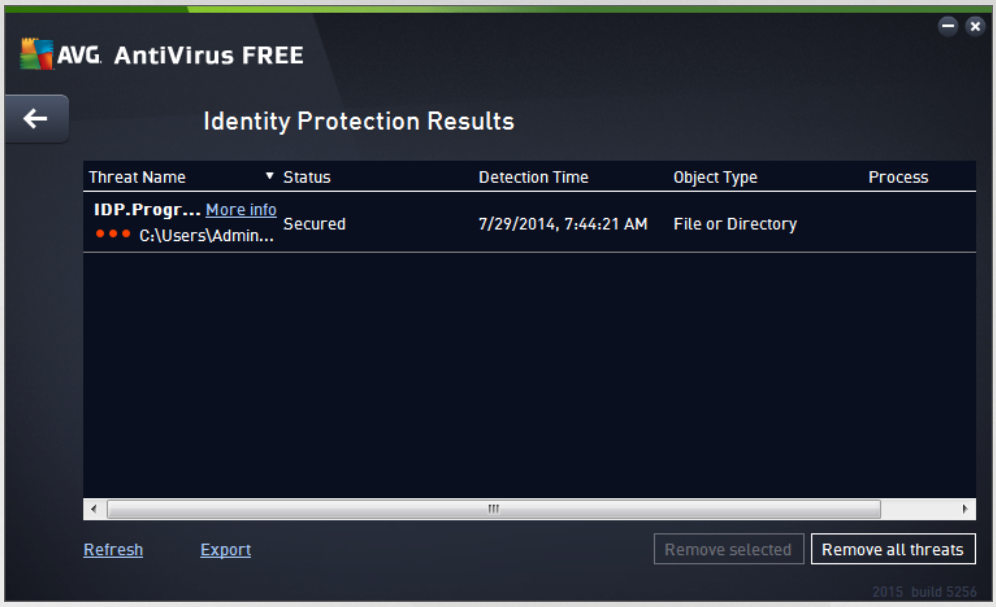
- ***Threat Name*** - description (*possibly even name*) of the detected object and its location; the *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia
- ***Status*** - action performed with the detected object
- ***Detection Time*** - date and time the threat was detected and blocked
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call up the potentially dangerous object so that it could be detected

Control buttons

- ***Refresh*** - update the list of findings detected by ***Online Shield.***
- ***Export*** - export the entire list of detected objects in a file.
- ***Remove selected*** - in the list you can highlight selected records, and use this button to delete just these selected items.
- ***Remove all threats*** - use the button to delete all records listed in this dialog.
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog.

13.3. Identity Protection Results

The ***Identity Protection Results*** dialog is accessible via the ***Options / History / Identity Protection Results*** menu item in the upper line navigation of the **AVG AntiVirus Free Edition 2015** main window.



The dialog provides a list of all findings detected by the Identity Protection component. For each detected object the following information is provided:

- ***Threat name*** - description *(possibly even name)* of the detected object, and its source; The *More info* link takes you to a page providing detailed information on the detected threat within the online virus encyclopedia
- ***Status*** - action performed with the detected object
- ***Detection time*** - date and time the suspicious object was detected
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call up the potentially dangerous object so that it could be detected

In the bottom part of the dialog, below the list, you will find information on total number of detected objects listed above. You can also export the entire list of detected objects in a file (***Export list to file***) and delete all entries on detected objects (***Empty list***).

Control buttons

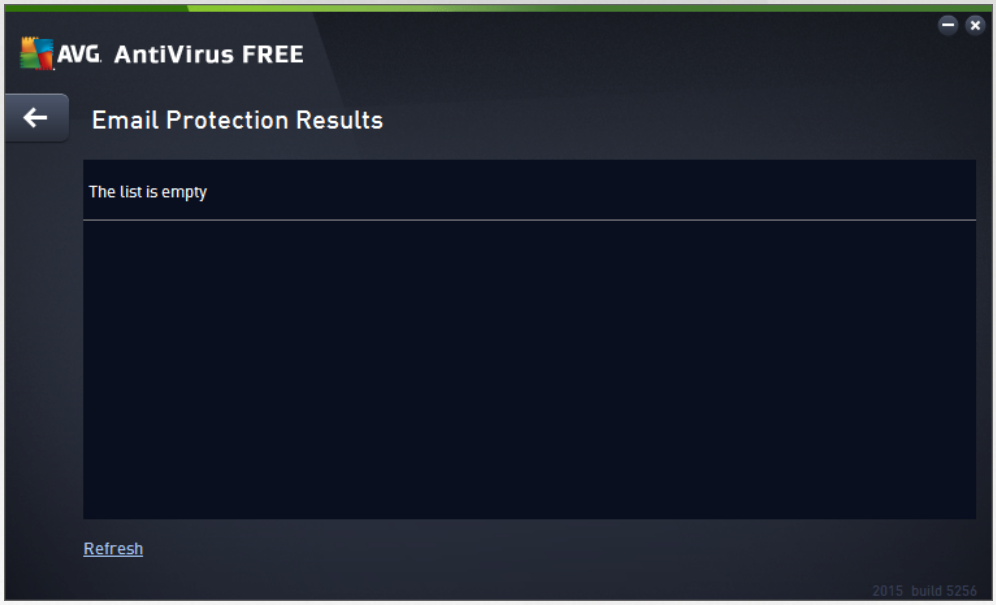
The control buttons available within the ***Identity Protection Results*** interface are as follows:

- ***Refresh*** - updates the list of detected threats.
- ***Export*** - export the entire list of detected objects in a file.

- ***Remove selected*** - in the list you can highlight selected records, and use this button to delete just these selected items.
- ***Remove all threats*** - use the button to delete all records listed in this dialog.
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog.

13.4. Email Protection Results

The ***Email Protection detection*** dialog is accessible via the ***Options / History / Email Protection detection*** menu item in the upper line navigation of the **AVG AntiVirus Free Edition 2015** main window.



The dialog provides a list of all findings detected by the Emails component. For each detected object the following information is provided:

- ***Detection Name*** - description *(possibly even name)* of the detected object, and its source
- ***Result*** - action performed with the detected object
- ***Detection Time*** - date and time the suspicious object was detected
- ***Object Type*** - type of the detected object
- ***Process*** - what action was performed to call up the potentially dangerous object so that it could be detected

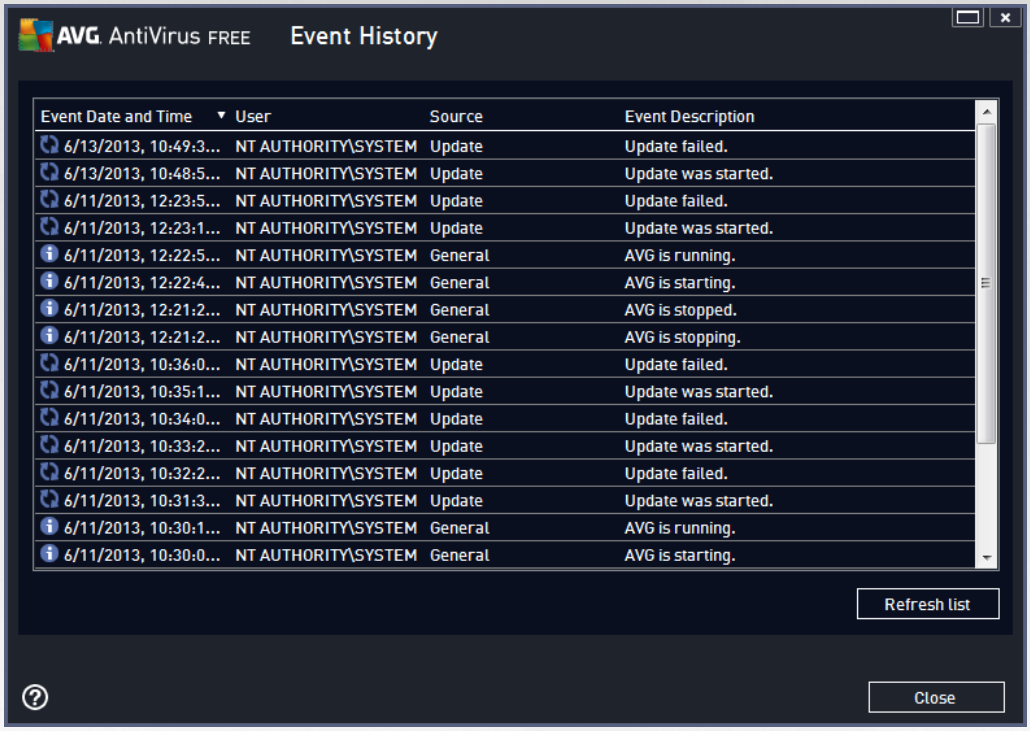
In the bottom part of the dialog, below the list, you will find information on total number of detected objects listed above. You can also export the entire list of detected objects in a file (***Export list to file***) and delete all entries on detected objects (***Empty list***).

Control buttons

The control buttons available within the ***Email Scanner detection*** interface are as follows:

- ***Refresh*** - updates the list of detected threats.
- ← - to switch back to the default AVG main dialog *(components overview),* use the arrow in the upper left-hand corner of this dialog

13.5. Event History


AVG AntiVirus FREE
Event History
Event Date and Time
User
Source
Event Description
6/13/2013, 10:49:3... NT AUTHORITY\SYSTEM Update Update failed.
6/13/2013, 10:48:5... NT AUTHORITY\SYSTEM Update Update was started.
6/11/2013, 12:23:5... NT AUTHORITY\SYSTEM Update Update failed.
6/11/2013, 12:23:1... NT AUTHORITY\SYSTEM Update Update was started.
6/11/2013, 12:22:5... NT AUTHORITY\SYSTEM General AVG is running.
6/11/2013, 12:22:4... NT AUTHORITY\SYSTEM General AVG is starting.
6/11/2013, 12:21:2... NT AUTHORITY\SYSTEM General AVG is stopped.
6/11/2013, 12:21:2... NT AUTHORITY\SYSTEM General AVG is stopping.
6/11/2013, 10:36:0... NT AUTHORITY\SYSTEM Update Update failed.
6/11/2013, 10:35:1... NT AUTHORITY\SYSTEM Update Update was started.
6/11/2013, 10:34:0... NT AUTHORITY\SYSTEM Update Update failed.
6/11/2013, 10:33:2... NT AUTHORITY\SYSTEM Update Update was started.
6/11/2013, 10:32:2... NT AUTHORITY\SYSTEM Update Update failed.
6/11/2013, 10:31:3... NT AUTHORITY\SYSTEM Update Update was started.
6/11/2013, 10:30:1... NT AUTHORITY\SYSTEM General AVG is running.
6/11/2013, 10:30:0... NT AUTHORITY\SYSTEM General AVG is starting.
Refresh list
Close

The ***Event History*** dialog is accessible via the ***Options / History / Event History*** menu item in the upper line navigation of the **AVG AntiVirus Free Edition 2015** main window. Within this dialog you can find a summary of important events that occurred during **AVG AntiVirus Free Edition 2015** operation. The dialog provides records of the following types of events: information about updates of the AVG application; information on scanning start, end, or stop (*including automatically performed tests*); information on events connected with virus detection (*either by the resident shield or scanning*) including occurrence location; and other important events.

For each event, the following information is listed:

- ***Event Date and Time*** gives the exact date and time the event occurred.
- ***User*** states the name of the user currently logged in at the time that the event occurred.
- ***Source*** gives information about a source component or other part of the AVG system that triggered the event.
- ***Event Description*** gives a brief summary of what actually happened.

Control buttons

- ***Refresh list*** - press the button to updates all entries in the list of events
- ***Close*** - press the button to return to the **AVG AntiVirus Free Edition 2015** main window

14. AVG Updates

No security software can guarantee true protection from various types of threats unless it is regularly updated! Virus writers are always looking for new flaws that they can exploit in both software and operating systems. New viruses, new malware, new hacking attacks appear daily. For this reason, software vendors are continually issuing updates and security patches, to fix any security holes that are discovered.

Considering all the newly-emerged computer threats, and the speed they spread, it is absolutely crucial to update your **AVG AntiVirus Free Edition 2015** regularly. Best solution is to stick to the program default settings where the automatic update is configured. Please mind that if the virus database of your **AVG AntiVirus Free Edition 2015** is not up-to-date, the program will not be able to detect the latest threats!

It is crucial to update your AVG regularly! Essential virus definition updates should be daily if possible. Less urgent program updates can be weekly.

14.1. Update launch

To provide maximum security available, **AVG AntiVirus Free Edition 2015** is by default scheduled to look for new virus database updates every four hours. Since AVG updates are not released according to any fixed schedule but rather in reaction to amount and severity of new threats, this check-up is highly important to make sure your AVG virus database is kept up-to-date all the time. If you want to check the new update files immediately, use the Update now quick link in the main user interface. This link is available at all times from any user interface dialog. Once you start the update, AVG will first verify whether there are new update files available. If so, **AVG AntiVirus Free Edition 2015** starts to download them and launches the update process itself. You will be informed about the update results in the slide dialog over the AVG system tray icon.

Unfortunately, within **AVG AntiVirus Free Edition 2015** the option of setting your own parameters of the update schedule is disabled *(so you cannot limit the number of update launches).*This configuration is only accessible in the paid AVG product version.

14.2. Update levels

AVG offers two update levels to select from:

- ***Definitions update*** contains changes necessary for reliable antivirus and anti-spyware protection. Typically, it does not include any changes to the code and updates only the definition database. This update should be applied as soon as it is available.
- ***Program update*** contains various program changes, fixes and improvements.

When scheduling an update, it is possible to define specific parameters for both update levels:

- Definitions update schedule
- Program update schedule

Note: *If a time coincidence of a scheduled program update and scheduled scan occurs, the update process is of higher priority and the scan will get interrupted. In such a case you will be informed about the collision.*

15. FAQ and Technical Support

Should you have any sales or technical trouble with your **AVG AntiVirus Free Edition 2015** application, there are several ways to look for help. Please chose from the following options:

- ***Troubleshooting in help file***: A new ***Troubleshooting*** section is available directly in the help file included in **AVG AntiVirus Free Edition 2015**. This section provides a list of most frequently occurring situations when a user desires to look up professional help to a technical issue. Please select the situation that best describes your problem, and click it to open detailed instructions leading to the problem solution.

- ***AVG website support center***: Alternatively, you can look up the solution to your problem on the AVG website (*http://www.avg.com/*). In the ***Support*** section you can find an overview of thematic groups dealing with both sales and technical issues, a structured section of frequently asked questions, and all available contacts.

- ***AVG ThreatLabs***: A specific AVG related website (*http://www.avg.com/about-viruses*) is dedicated to virus issues providing structured overview of information related to online threats. You can also find instructions on removing viruses, spyware, and advice on how to stay protected.

- ***Discussion forum***: You can also use the AVG Free users discussion forum at http://forums.avg.com.

Unfortunately, using AVG AntiVirus Free Edition 2015 you are not entitled to technical support provided to full versions of AVG products. You may want to consider buying the full version of AVG, then please visit the AVG website (http://www.avg.com/) for information on AVG 2013 paid products purchase options.